



Strengthening Cybersecurity in Digital Transformation

by

Harrison Stewart

Thesis

Submitted to Flinders University

for the degree of

Doctor of Philosophy

College of Science and Engineering

October 2023

Table of Contents

- Table of Contents..... 2
- List of Abbreviations..... 7
- Executive Summary.....8
- Declaration.....11
- Acknowledgement..... 12
- Statement of Authorship..... 13
- Chapter 1. Introduction..... 14
 - 1.1. Overview..... 14
 - 1.2. Background to the Research.....14
 - 1.3. Research Topic..... 16
 - 1.4. Aims and Objectives of the Study.....17
 - 1.5. Contribution of the Research..... 19
 - 1.5.1. Theoretical contributions..... 19
 - 1.5.2. Methodological contributions..... 21
 - 1.5.3. Practical contributions.....22
 - 1.5.4. Assessing the contribution..... 22
 - A. What is the subject of this study?..... 22
 - B. How? The clarity of the argument relies on the persuasiveness of the premises and the evidence that supports them..... 23
 - C. Why is this being studied now?..... 24
 - D. Significance.....24
 - 1.6. Structure of Thesis.....25
 - 1.7. References..... 33
- Chapter 2. Literature Review
(Theoretical Background).....41
 - 2.1. Digital Transformation..... 42
 - 2.2. Financial Technology (FinTech)..... 44
 - 2.3. Cloud computing..... 46
 - 2.4. Information Security Management..... 49
 - 2.5. Information Security Policy..... 51
 - 2.6. Technical Acceptance Model..... 54
 - 2.7. Cybersecurity as social problem..... 56
 - 2.7.2. Socio-Technical System Theory Approach to Information Security (STS).....57
 - 2.8. NFC Model.....59
 - 2.9. Literature Summary.....64

- 2.10. The Nine Five Circle (NFC) Model..... 65
 - 2.10.1. Development of the NFC Model..... 66
 - 2.10.1.1 Stage 1: Situational Awareness (SA)..... 66
 - a. Assets Protection..... 69
 - b. Information security policy (ISP) and governance..... 69
 - 2.10.1.2 Stage 2: Integration Control..... 70
 - Cybersecurity programme..... 72
 - Risk Assessment..... 74
 - Risk Treatment..... 74
 - 2.10.1.3. Stage 3: Gap Closure..... 75
- 2.11. NFC Model validation..... 77
 - 2.11.1. Observation..... 77
 - 2.11.2. Evaluation..... 77
 - 2.11.3. Reliability and Validity at Post-fieldwork Stage..... 78
 - 2.11.3.a. Reliability..... 78
 - 2.11.3.b. Validity..... 78
- 2.12. NFC Summary..... 78
- 2.13. References..... 80
- Chapter 3. Methodology..... 100
 - 3.1. Overview..... 100
 - 3.2. Research Design..... 100
 - A. Qualitative Phase (Exploratory Research)..... 102
 - B. Quantitative Phase (Descriptive & Casual Research)..... 102
 - 3.3. Qualitative Research Methods Step..... 104
 - 3.3.1. Overview..... 104
 - 3.3.2. Case Studies..... 104
 - 3.3.3. Interviews..... 105
 - 3.3.4. Observation..... 109
 - 3.4. Quantitative Research Step..... 109
 - 3.4.1. Overview..... 109
 - 3.4.2. Levels of Theory, Measurement and Statistical Evaluation..... 110
 - 3.4.3. Data Collection Method..... 111
 - 3.4.4. Questionnaire Design..... 111
 - 3.4.5. Scales and Measurement..... 113
 - 3.4.6. Operationalisation of Constructs..... 113
 - 3.5. Statistical Analysis..... 114
 - 3.5.1. Overview..... 114
 - 3.5.2. Exploratory Factor Analysis..... 114
 - 3.5.3. Confirmatory Factor Analysis..... 115

3.5.4. Structural Equation Modelling.....	116
3.6. Chapter Summary.....	116
3.7. References.....	117
Chapter 4. STUDY I: Data security and consumer trust in FinTech innovation.....	119
Chapter 5. STUDY 2: The hindrance of cloud computing acceptance within the financial sectors in Germany.....	154
Chapter 6. STUDY 3: Security versus compliance: an empirical study of the impact of industry standards compliance on application security.....	184
Chapter 7. STUDY 4: Digital transformation security challenges.....	229
Chapter 8. STUDY 5: Information security management and the human aspect in organisations.....	273
Chapter 9. STUDY 6: A systematic framework to explore the determinants of information security policy development and outcomes:.....	321
Chapter 10. Conclusion.....	362
10.1. Overview.....	362
10.2. Theoretical Contribution.....	363
10.3. Methodological Contribution.....	365
10.4. Managerial Implications.....	366
10.5 Discussion.....	370
10.6 Limitations and future research.....	374
10.7 Chapter Summary.....	375
10.8 References.....	376
Chapter 11.	
Appendix.....	396
11.1 PAPER 1.....	396
11.1.1 Value Added Justification.....	396
11.1.2 Customer's Trust Justification.....	397
11.1.3 Data Security Justification.....	398
11.1.4 User Interface Design (UI) Justification.....	399
11.1.5 FinTech Promotion Justification.....	400
11.2 Basis of Assumption.....	401
11.3 PAPER 2.....	402
11.3.1 Banks in Germany's intention to adopt IaaS are not always influenced by the organisational factor (Justification).....	402
11.3.2 Consumer trust does not always influence organisations' intention to adopt cloud platforms (IaaS) (Justification).....	403
11.3.3 The willingness of banks in Germany to trust IaaS is not influenced by data security (Justification).....	404
11.3.4 Data security does not influence banks in Germany's intention to adopt IaaS (Justification).....	404
11.3.5 Banks in Germany' intention to adopt IaaS is not influenced by the technological factor (Justification).....	405

11.3.6 Technological factors do not influence the willingness of banks in Germany to adopt IaaS (Justification)..... 406

11.3. 7 Environmental factors are not a vital determinant of consumer trust in banks' intention to adopt IaaS (Justification)..... 407

11.4 PAPER 4..... 408

11.5 References:..... 410

List of Figures and Tables

Figures

Figure 1. Objectives of the research..... 7
Figure 2. Framework of thesis..... 7
Figure 3. NFC Information Security Management System Model..... 7
Figure 4. NFC Integration Phase with Application Security.....7
Figure 5. Flowchart depicting the research design..... 7

Tables

Table *. List of abbreviations..... 2
Table *. List of abbreviations..... 2
Table 1. Demographic of digital products users' participants..... 2
Table 2. Table 2. Industrial participants and key informants.....2
Table 3. Demographics of respondents based on educational level.....2
Table 4. Table of authorship.....2

List of Abbreviations

Abbreviations	Items
IS	Information Systems
DT	Digital Transformation
NFC	Nine Five Circle / Nine-Five-Circle
CIA	Confidentiality, Integrity, Availability
SEM	Structural Equation Modelling
A	Cronbach's Coefficient Alpha
-test	Student's t-test
AMOS	Analysis of Moment Structures
CFA	Confirmatory Factor Analysis
ICT	Information and Communications Technology
CFI	Comparative Fit Index
TLI	Tucker Lewis Index
TAM	Technology Acceptance Model
TOE	Technological, Organisational and Environmental
PEOU	Perceived Ease of Use
UTAUT	Unified Theory of Acceptance and Use of Technology
IT	Information Technology
NIST	National Institute of Standards and Technology
ISO	International Organisation for Standardisation
STS	Socio-Technical System Theory Approach to Information Security
GRC	Governance, Risk, Compliance
CDI	Constrained Data Items
SaaS	Software as a Service
IaaS	Infrastructure as a Service
PaaS	Platform as a Service

Executive Summary

Digital transformation (DT) and information systems (IS) have opened new markets, resources and capabilities for organisations that use and depend on technologies such as artificial intelligence (AI), Industry 4.0, Big Data, robotics, the Internet of Things (IoT) and blockchain. However, digitalization also leads to new cybersecurity issues related to DT strategies that use these advanced technologies. Approaches to strengthen cybersecurity during DT require better insight, given the paucity of empirical evidence on the key factors that support cybersecurity during DT. DT strategy involves technological and human activities, increasing cybersecurity's complexity during DT. As a result of this complexity, organisations are hesitant to implement DT, knowing that cyberattacks on DT can cause devastating social, organisational, and economic damage.

The study analysed the factors that improved security in the DT environment and proposed a model that strengthens secure digitalization. The result of the study was the development of a new cybersecurity model called the Nine Five Circle (NFC). The NFC model combines IS and DT security uniquely.

A novel methodology that supported empirical testing of cybersecurity analysis was achieved in this study by including qualitative and quantitative methods. The research included a qualitative exploratory stage, followed by quantitative descriptive and causal studies. The qualitative exploratory phase used case studies and semi-structured interviews to gather data from innovative sector stakeholders and produce operational constructs, variables, and definitions. This exploratory stage revealed significant variables and correlations used to develop the conceptual framework, the research instruments, and the hypotheses for the quantitative phase. The exploratory design was crucial to achieving a holistic, in-depth analysis across multiple sectors. Descriptive research was essential for calculating variances and meant to define proportions, characteristics and relationships between the variables identified in the exploratory phase. For the causal phase of the study, the identified variables were categorised into measurable dependent and independent variables. By organising the variables into constructs, it becomes possible to explain and predict. This final stage of causal research was required to determine security challenge factors obstructing successful DT and IS strategies. Patterns and trends were identified using factor analysis and structural equation modelling with pattern matching in case studies.

Additionally, organisations that rely solely on technical solutions without considering human factors are creating a gap in the relationship between humans and technology, and this research has demonstrated that humans still need to be improved in cybersecurity. As humans and technology interact, a complex system emerges, posing more significant challenges in resolving cybersecurity issues. The NFC model assisted in addressing significant cybersecurity issues faced by traditional organisational structures when implementing DT and IS security strategies.

This research has helped to fill a gap in the IS and DT literature where the security aspect of DT implementation requires attention. This study adds to the understanding of cybersecurity management issues in DT.

The findings indicate that cybersecurity can be improved in the context of DT by focusing on the following key elements: (i) security misperception, (ii) threat vulnerability and risk assessment, (iii) cybersecurity strategy, (iv) development of secure information systems, (v) security audit and assessment, (vi) protection monitoring, (vii) strategic advanced threat analysis, (viii) incident response and remediation, (ix) managers and stakeholders involvement, (x) information security and cybersecurity investments, (xi) information security policies, (xii) application security policies, (xiii) information security facilitators, (xiv) security training, (xv) commitment, and (xvi) external partners. These constructs were operationalized, validated qualitatively and quantitatively, and processed in the NFC cybersecurity enhancement model. The tested model contributes to the theoretical advancement of the IS and DT cybersecurity analysis layers.

The study results also show management behaviours necessary to implement strengthened cybersecurity for DT: i) managers' commitment to security support, ii) the need to invest in security programs, iii) implementing in-depth security measures, iv) creating a security-aware culture and trust, v) improving security-awareness training, and vi) implementing cybersecurity policy and governance. The DT era presents both unprecedented opportunities and challenges for organisations. While digital technologies like AI, Industry 4.0, Big Data, robotics, IoT, and blockchain provide innovative resources and skills, they also introduce new cybersecurity issues. During DT, it is crucial to enhance cybersecurity measures. This study proposes an NFC model integrating information and DT security. The model was validated using qualitative and quantitative methods. This research contributes to understanding

cybersecurity management issues in DT and adds to the theoretical advancement of the IS and DT cybersecurity analysis layer. The study's results highlight the crucial management behaviours necessary to implement strengthened cybersecurity for DT. By addressing the core constructs identified in this study, managers can better protect their organisations from the devastating effects of cyberattacks during DT. This study provides valuable insights for organisations and policymakers seeking to implement successful cybersecurity strategies during DT. Organisations must have the necessary structures, resources, and plans to mitigate cybersecurity risks and, therefore, must recognize that security is an essential aspect of their business strategy.

Declaration

This work does not contain any material previously accepted for the attainment of a degree or qualification at any university or other educational institution. To the best of my knowledge and belief, I have written the material contained in the thesis myself and published it as part of this thesis. I have also referred to previously published papers in the body of the thesis.

Acknowledgement

I would like to express my gratitude to God for His Mercy and Grace in everything. I am incredibly grateful to my supervisor, Prof. Giselle Rampersad, for her wise advice, constant support, and tolerance during my doctoral studies. My parents, sisters, children, and my family deserve my sincere gratitude. Without their incredible patience and support over the past years, I would not have been able to complete my studies.

Statement of Authorship

I am the sole author of all contributions, except for two contributions, to which I hereby express my gratitude in the following table:

Nr	Paper	Author	Co-Author
1	Data security and consumer trust in FinTech innovation in Germany	Harrison Stewart (99%)	Jan Jürjens (1%)
2	The hindrance of cloud computing acceptance within organisations.	Harrison Stewart (100%)	
3	Security versus compliance: an empirical study of the impact of industry standards compliance on application security	Harrison Stewart (100%)	
4	Digital Transformation Security Challenges	Harrison Stewart (100%)	
5	Information security management and the human aspect in organisations	Harrison Stewart (99%)	Jan Jürjens (1%)
6	A systematic framework to explore the determinants of information security policy development and outcomes	Harrison Stewart (100%)	

Chapter 1. Introduction

1.1. Overview

This research has developed a model to enhance IS security and DT, as outlined in section 1.2. The primary objective is to identify the critical factors that can improve cybersecurity and how they can lead to successful DT, which is discussed in section 1.3. Furthermore, the research explores the link between IS and DT, which contributes to advancing theory development in these fields, as explained in section 1.4. This study also provides practical insights for management to effectively enhance their organisations' security posture and DT strategies, as discussed in section 1.5.

1.2. Background to the Research

The concept of DT entails implementing changes throughout an organisation's management and IT infrastructure in response to external developments, according to Berman (2019). This topic is receiving significant attention from researchers and practitioners, likely due to evidence suggesting a positive correlation between DT and enhanced organisational performance (Jonathan, 2019). Existing literature indicates that integrating new DT into an organisation's current IT infrastructure and business processes, aligned with overall goals, can yield benefits. Empirical studies also reveal that successful DT can enhance communication among suppliers, collaborators, and partners, adding value (Stewart & Jürjens, 2018; Al-Kaabi, 2010; Matt, 2015).

DT has enabled organisations to collect and use data more effectively, giving them a competitive edge (Ifinedo, 2014; Imgrund et al., 2018). However, implementing new technologies requires careful planning and execution to achieve the benefits, as pointed out by Vial (2019). Researchers have identified three areas of concern: technology, organisational structure and management (Agrawal et al., 2013; Soomro et al., 2016). However, a closer study reveals that information security is a common issue in addition to the three areas that pose a challenge in many DT initiatives (Lallie et al., 2021, Auyorn et al., 2020). As organisations increasingly rely on IT to conduct their operations, they have become more vulnerable to cyberattacks and information security breaches (Collet, 2020; Karpunina et al., 2019; Lundgren & Möller, 2017). According to NIST, any malicious activity that attempts to capture, disrupt, deny, impair or destroy information system resources or the information itself is called a cyberattack (NIST SP 800-12 Rev). Both cyberattacks and information security breaches are primary concerns, as such breaches can lead to significant financial losses.

Previous research has focused on information security as a technological problem (Jonathan, 2019; Foerster-Metz et al., 2018). In order to address these challenges, technical solutions such as firewalls and perimeter protection are often implemented (Soomro et al., 2016). However, researchers argue that in the new era of digitalisation, management and organisational factors must be recognised to meet the growing demands for information security (Agarwal, et al., 2010; Moon et al., 2018). Other studies and institutions have shown that organisations can reduce cyberattacks by implementing cybersecurity systems and strategies to protect critical systems and sensitive information from digital attacks through technology, human and processes (Bakar et al., 2021; García-García et al., 2021; Khan et al., 2022; M'baya et al., 2017; Tervoort et al., 2020).

According to the NIST definition of cybersecurity, cybersecurity includes preventing the unauthorised use and exploitation of electronic information and communication systems and ensuring confidentiality, integrity and availability (Lallie et al., 2021, Auyporn et al., 2020). On the other hand, ISO/IEC 27001 serves as an international standard for information security that describes the requirements for an effective information security management system (ISMS) that improves systems' confidentiality, integrity and availability. ISO (2018, p. 4), added validity, non-repudiation and authenticity. Confidentiality ensures the privacy of sensitive data by restricting access to authorised individuals (Collet, 2020). Integrity ensures that data is correct and accurate and cannot be altered by unauthorised users during transmission or storage (Collet, 2020; Karpunina et al., 2019). Availability ensures that authorised users can access data or services at any time (Karpunina et al., 2019; Lundgren & Möller, 2017). Validity refers to the consistency of data or information according to predefined rules, while authenticity aims to confirm that a digital object is what it claims to be (Collet, 2020; Stewart & Jürjens, 2017). Non-repudiation assures that the truth of something cannot be disputed (Karpunina et al., 2019; Lundgren & Möller, 2017; Stewart, 2022). Ensuring these security measures is crucial in protecting company data and mitigating cyber threats.

Considering humans, processes and technology, ISO 27001 provides an approach to managing an organisation's information security. The standard covers various aspects of information security management, including establishing, implementing, maintaining, and continuously improving an ISMS, and applies to organisations of all sizes, types, and kinds. Building on this, a company's digital practices should guide its DT strategy and encompass technological and human activities throughout the lifecycle. Therefore, future studies on DT should examine how factors such as digital strategy,

organisational culture, humans, and business processes can impact information security (Agarwal et al., 2010; Tu et al., 2018).

Stewart (2017) develops the NFC model to address DT cybersecurity challenges. The NFC model considers noteworthy factors from past literature, identifies significant challenges, and presents a strategic process to mitigate those challenges. Stewart has used this model in several works (Stewart & Jürjens, 2017; Stewart & Jurjens, 2018; Stewart, 2022).

In 2021, Stewart proposed that the type and size of an organisation should not measure its cybersecurity and information protection effectiveness but instead by the characteristics of the activities that enhance cybersecurity and improve DT, such as content focus, coherence, and duration. In his recent work, Stewart (2022) implemented the NFC model, which features six critical elements to increase managers' perception, change practice, and improve cybersecurity outcomes: (a) cybersecurity content focus, (b) secure coding, (c) coherence, (d) cybersecurity investment, (e) information security policy and compliance and (f) ongoing professional development with IT groups.

To fill the research gap in IS literature, six published papers, including Stewart's 2017 NFC model, were reviewed, and analysed alongside other IS research. The results of this analysis led to the creation of a cybersecurity model called NFC cybersecurity. This model includes strategic planning, essential concepts, and success factors and is designed to help organisations overcome cyber-attack challenges while achieving their DT goals securely.

1.3. Research Topic

Companies and cultures are being transformed by technological advancements, which are changing how businesses compete and create value. The recent DT movement has increased organisations' reliance on advanced technologies such as Industry 4.0, robots, the Internet of Things (IoT), artificial intelligence (AI), cloud computing, predictive analytics, blockchain, and Big Data. While digitization offers benefits such as opening new markets, skills, and resources (Barringer & Harrison, 2000; Wilkinson et al., 2004), it can also pose challenges, such as the rise of cybercrime (Burns et al., 2001; Karumbaiah et al., 2016; Shahri et al., 2012; Stewart & Jürjens, 2018). These challenges have been described as obstacles by Stewart (2022) to adopting DT. Therefore, a secure and efficient approach is essential for DT.

1.4. Aims and Objectives of the Study

This research aims to explore information and cyber security challenges in organisations' DT and proposes a model called NFC for managing information and cyber risks. The main objective, illustrated in Figure 1 of this study, is to

1. Empirically analyse the key factors influencing the adoption of DT (e.g., FinTech).
2. Empirically analyse the critical factors influencing cloud computing for data storage and processing (e.g., Infrastructure as a Service).
3. Identify the key sources of cyber and information risk, both internal and external, during application development.
4. Explore organisational initiatives that help technology companies manage information and cyber risks.
5. Develop a novel cybersecurity model called NFC that can be used to mitigate DT's cybersecurity problems.
6. Apply the NFC model to study the determinants of information security policies and outcomes in organisations.
7. Apply the NFC to develop practical recommendations to improve the cyber risk management process of technology companies.

This thesis aims to address and answer the following research question:

1. What are the main factors contributing to the adoption of cloud computing?
2. What are the potential cybersecurity vulnerabilities associated with cloud computing, and what factors hinder its adoption?
3. To what extent does a company's adherence to an industry standard such as ISO27001 influence its software development cybersecurity strategy?
4. What are the main DT challenges, and how can they be overcome?
5. To what extent can organisations protect themselves from malicious attacks, data breaches and unauthorised control that could compromise critical infrastructure or personal security?
6. What systematic approach can organisations take to developing and implementing an information security policy during DT?

The answers to these questions are reflected in each of the six published papers in this work.

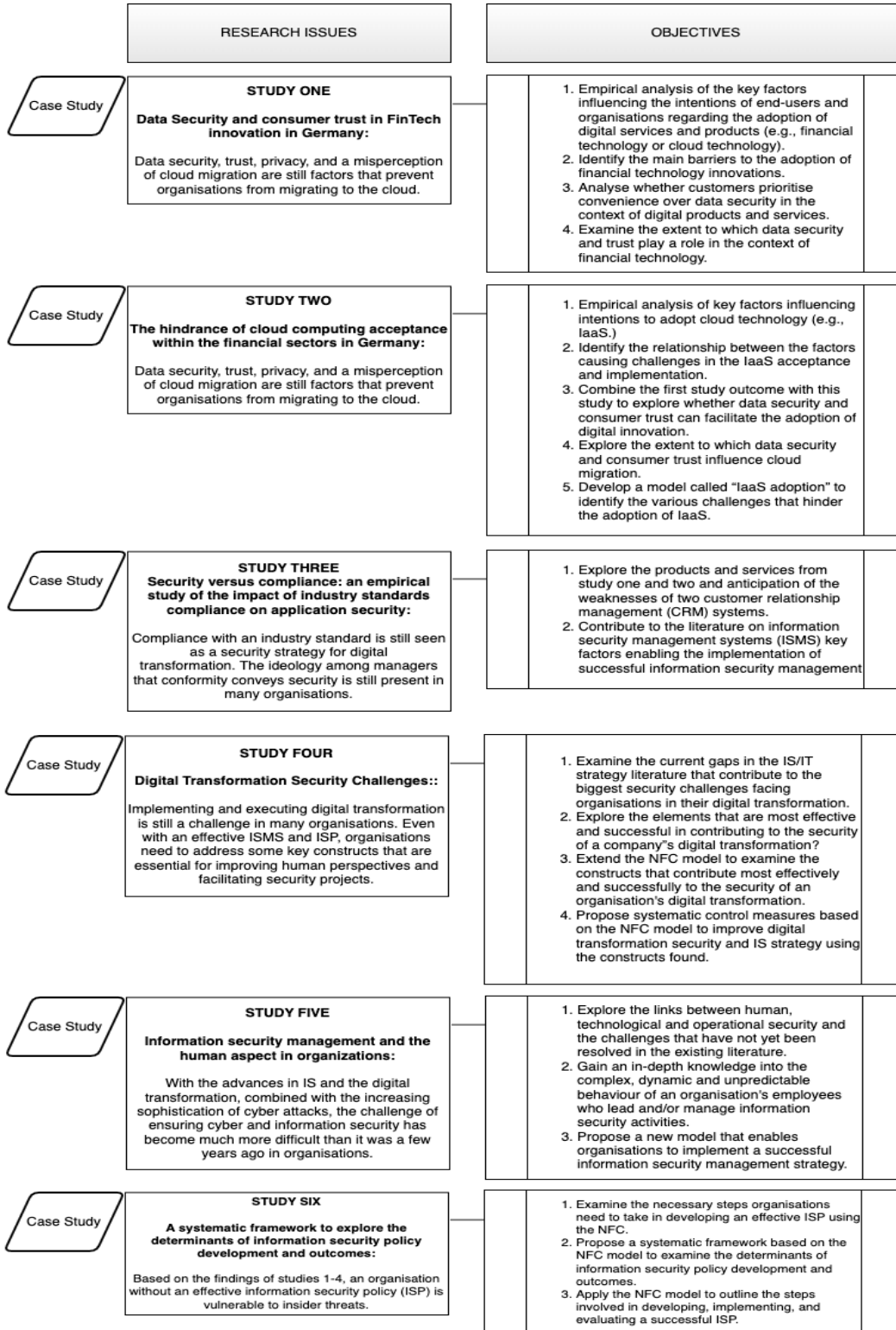


Fig. 1. Objectives of the research

1.5. Contribution of the Research

This section focuses on the contributions of this dissertation. The section is divided into three subsections addressing contribution to theory, methodology and practice (Holweg et al., 2015).

1.5.1. Theoretical contributions

This research makes a significant contribution as it develops a novel cybersecurity model called NFC, a comprehensive framework that combines theories from cybersecurity (Bongiovanni, 2019), risk management (Shareeful et al., 2017), and DT (Hess et al., 2016). This model provides an innovative approach to secure DT initiatives. It integrates human factors (Abualoush et al., 2018; Andriotis et al., 2015), technology (Alhabeeb et al., 2010) and processes to ensure optimal security (Stewart & Jürjens, 2017).

Over the years, numerous articles have been published on DT innovation, often called "state-of-the-art" pieces. These articles, including works by Hevner et al. (2004, p. 77), Halbrecht (1977), Gartner (2019), Morakanyane et al. (2017), Hess et al. (2016), and Gomber et al. (2018), review and critique the current state of theory. Many of these articles suggest future research directions, outlining agendas or visions for the field, and some even provide criteria for assessing the quality of research. The articles mentioned earlier explicitly highlight aspects that should be considered moving forward but neglect the aspect of cybersecurity in these innovations. Despite the importance of research in IS, studies on DT security have largely been neglected.

Numerous cybersecurity literature has also mainly focused on organisational security culture, with little attention paid to DT cybersecurity challenges (Bongiovanni, 2019; Yilmaz & Yalman, 2016; FireEye, 2015; Unit-Department, 2019). Those who have looked at DT security have focused on specific aspects without considering the full range of factors required to improve cyber security in the DT context (Wangen, 2019). Although organisational IT security research is an essential subfield in IS, it is often focused on specific industry sectors (Kwon & Johnson, 2014; Yang & Lee, 2016). As a result, most DT security seems to have been overlooked (Eurostat, 2015). Previous studies have examined the impact of cybersecurity characteristics on IS or technology adoption (Stewart & Jürjens, 2018; Cragg et al., 2011; Arendt, 2008). However, there needs to be more research on the impact of cybersecurity traits on IS security.

As per Sheehan et al. (2019), cyber vulnerabilities can lead to significant business risks, such as interruption in operations, loss of privacy, and financial losses. Maleks et al. (2020) state that inadequate cybersecurity can cost the global economy around USD 945 billion in 2020. Conklin (2014) highlights that identifying security threats in DT is critical and requires thorough knowledge of security-based technologies. Kazemi (2012) categorises security into three areas: computer security, information security and cyber security. Fielder et al. (2016) state that protecting organisations from potential cyber-attacks has become increasingly difficult (Fielder et al., 2016). Baker's (2007) work focuses on tackling cybersecurity challenges in organisations.

Goel & Chengalur (2010) highlight the problem of non-compliance by individuals with IT-related information security policies. Wang et al. (2008) focused solely on technical measures for enhancing an organisation's cybersecurity without considering the human factor. Although there are studies on implementing and utilising IT-related initiatives in developing countries, less attention has been paid to DT cybersecurity challenges in the context of global integration. Therefore, this study argues that IS research should fully consider the distinctive qualities of DT cybersecurity challenges holistically.

A key question arising from this discussion is how organisations can effectively implement strong cybersecurity measures during DT (Alhogail et al., 2014). Answering this question will help identify the impact of internal and external cybersecurity challenges on the digital transformation process and the barriers that may prevent decision-makers from being fully engaged (Nazareth & Choi, 2015).

This study combines six published papers revealing that mature cybersecurity initiatives can enhance an organisation's core productive activities with greater visibility and support. Management involvement and stakeholder acceptance are crucial for the success of cybersecurity models or strategies. Therefore, efforts to secure DT are more promising when all stakeholders show interest and support, leading to a secure DT process within their organisation (Rees et al., 2011). Therefore, this study makes theoretical and empirical contributions to enhance DT cybersecurity using a novel NFC model in a holistic approach to address and mitigate these challenges. This model integrates cybersecurity challenges with traits identified in current IS research and hypotheses of how these restrict DT security decisions (Wang et al., 2008; Muehe & Drechsler, 2017). The model is developed using the combined findings from the six published papers.

The sociology of translation application, such as problematisation, interessement, recruitment and mobilisation, helps to analyse the results of the six papers (Alvesson & Sandberg, 2011). The participation of managers and decision-makers in a cybersecurity initiative is driven by problematisation and interest if they perceive the initiative as a solution to their challenges (Alvesson & Sandberg, 2011). There is interessement in a solution if it is pragmatic and can effectively solve the problem. This attracts the interest of managers and decision-makers and gains their support for the proposed solution (Rodon et al., 2008). Hence, interest is a fundamental prerequisite for the successful adoption and use of the initiative with positive potential expectations. The above paragraph suggests that it would be prudent to explore how involvement of initiators, IT professionals, managers, and decision makers in cybersecurity initiatives can facilitate and improve DT.

The effectiveness of the NFC model is validated through case studies and empirical research. The theoretical underpinnings of the model have also been validated by empirical data demonstrating its potential to provide reliable cybersecurity solutions for DT initiatives (Yin, 2018). In this work, all case studies were conducted in various sectors. This model's results can guide organisations to improve their IS security tactics to promote the secure innovation, adoption, and use of digital technologies.

1.5.2. Methodological contributions

The main objective is to explore the various cybersecurity challenges related to DT and to contribute to the existing literature on IS research (Weishäupl et al., 2015). Ultimately, the study aims to develop a cybersecurity model to secure DT effectively (Myers, 1997).

The study made a methodological contribution in two ways. First, a case study strategy and an interpretive approach to data collection were applied, which may be helpful for future studies on the adoption and implementation of security-related IS initiatives in organisations and communities in the context of digital transformation. Second, the techniques used for data collection provide valuable lessons that can be useful for similar studies (Walsham, 2006; Witmer et al., 1999).

A crucial aspect of a methodological contribution is whether applying theoretical concepts and models developed in different contexts is appropriate. It is debatable whether research theories and models formulated in one country are appropriate for studies in another country due to differences in social and cultural context. Using these theories in this research helps interpret case studies from various sectors by providing case studies (Yin, 2014).

1.5.3. Practical contributions

The six published papers from this research provide valuable insights into the practical implications of security-related DT initiatives. Cybersecurity initiatives must be integrated with the productive activities of organisations. Therefore, it is essential to comprehend the potential damage a cyberattack can cause to implement cybersecurity initiatives effectively. This understanding can help organisations prioritise and invest in improving their DT cybersecurity culture, thereby enhancing their security posture. It is evident from the six papers that IT professionals and managers need to adopt new approaches to persuade stakeholders of the urgency of improving their cybersecurity culture and its impact on their DT initiatives. One practical contribution is the NFC model, which simplifies all challenges to gain a holistic understanding of how variables interact and applies these insights holistically to arrive at a solution. This research explores how the DT initiative can be secured and its contribution to the IS literature, using the NFC model as a practical tool (Yildirim et al., 2011).

1.5.4. Assessing the contribution

Whetten (1989) outlined four crucial elements to consider while making a theoretical contribution. These elements include: (a) What is the subject of study? (b) How is it studied? (c) Why is it being studied? (d) Who, where, and when are involved (significance)? These questions define the scope for generalisation. Hence, a set of questions based on Whetten's framework can be employed to assess the theoretical contribution of this study. The study makes three significant contributions. Firstly, it reviews relevant literature on the relationship between DT initiatives, adoption, and cybersecurity. Secondly, the study provides rich empirical insights through six papers and introduces a novel cybersecurity model for analysing the cybersecurity challenges associated with DT initiatives. This model can guide the process of enhancing cybersecurity in DT and help address gaps in IS research. Thirdly, the study combines and applies different theories to enhance DT cybersecurity. Furthermore, other researchers conducting comparable studies in different countries can benefit from this study's fieldwork description and data techniques.

A. What is the subject of this study?

This study proposes a new cybersecurity model that can be used to improve the cybersecurity of DT initiatives. The NFC model, which is presented in section 2.10, can serve as a practical tool to guide the implementation process. The study also highlights the need for managers in IT industries to develop new strategies and knowledge to enhance cybersecurity.

B. How? The clarity of the argument relies on the persuasiveness of the premises and the evidence that supports them.

The research problem was examined in the first chapter of the paper from six different perspectives, including financial technology, cloud computing, DT challenges, information security policy, information security management systems, and software security. The results of the six studies were also examined from several theoretical angles, including (i) security misperception, (ii) threat vulnerability and risk assessment, (iii) cybersecurity strategy, (iv) development of secure information systems, (v) security audit and assessment, (vi) protection monitoring, (vii) strategic advanced threat analysis, (viii) incident response and remediation, (ix) managers and stakeholders involvement, (x) information security and cybersecurity investments, (xi) information security policies, (xii) application security policies, (xiii) information security facilitators, (xiv) security training, (xv) commitment, and (xvii) external partners (Wang et al., 2013).

Chapter 2 introduced the research topic and conducted a broadly relevant literature review. This chapter provided background information on the DT and cybersecurity context. Finally, this thesis logically reviewed different theories, forming its theoretical basis.

The interpretive approach and case study strategy were chosen to conduct the study, which was covered in detail in the third chapter's discussion of the research methodology.

To examine the connection between digital transformation initiatives and cybersecurity difficulties, Chapter 4 and 5 developed new cybersecurity models. Based on interpreting case study results from all six papers, chapters 6, 7, 8, and 9 further examined this model. Chapter 10 comes to a research conclusion that is backed up by credible data from the six papers.

The paper emphasises the significance of preventing cyber-attacks on digital transformation (DT) holistically and how it is crucial for organisations. It highlights that the barrier to cybersecurity contributes to the unwillingness to adopt digital transformation products and services. Empirical studies were conducted in various sectors, and their results were analysed based on the theories presented in the paper to develop a model for analysing cybersecurity challenges. In each of the six studies, conceptual frameworks were developed, namely the intention to adopt fintech, the intention to adopt cloud computing, the security of digital strategies, and information security policy. The index of terms and the glossary provide a convenient way to quickly find and understand the main concepts presented in this thesis.

C. Why is this being studied now?

Several organisations have experienced cyber-attacks on their digital initiatives, leading to the need for empirical studies to address these cybersecurity challenges. Many scholars in the field of IS are exploring the strategies organisations should use to address the cybersecurity challenges they encounter. This study emphasises the importance of a holistic cybersecurity solution, contributing to the ongoing debate on a new approach to implementing cybersecurity initiatives in organisations across various sectors (Schatz & Bashroush, 2017).

D. Significance

This work may interest innovative countries where disruptive technologies are at the peak of their development. It may also interest IS practitioners, decision-makers, managers, and policymakers implementing DT-related initiatives (Siponen, 2005).

Due to the enormous impact DT has on businesses (Bekkhus, 2016; Bharadwaj et al., 2013; Matt et al., 2015), significant cybersecurity risks need to be closely examined. Despite its benefits, it poses potentially severe cybersecurity risks due to the enormous amounts of processed data (Bassett et al., 2021). The entry points for cyber-attacks are becoming more comprehensive as more internet-connected devices, apps, and endpoints exist (Modi et al., 2012; Coppolino et al., 2016; Ramachandran, 2015).

In addition, the findings of this research shed light on emerging cyber risks (Bassett et al., 2021) and evolving attack strategies that are critical for organisations to update their cybersecurity measures and develop new tactics to combat these threats (Mehrban et al., 2020). The risks associated with different parts of DT, such as cloud migration, IoT adoption, and the application of AI and machine learning, need to be carefully considered (Modi et al., 2012; Coppolino et al., 2016; Ramachandran, 2015).

Furthermore, this research aims to identify the best approaches for integrating cybersecurity into DT (Mehrban et al., 2020). The practices recommended in this paper can serve as a reference for organisations aiming to secure their digital efforts efficiently. They can also serve as a guide to acquire a comprehensive knowledge of compliance standards and ensure that DT projects meet various regulatory requirements (e.g., in industries with stringent compliance laws) (Taylor et al., 2020). Organisations evaluating the cost-benefit ratio of various cybersecurity investments and methods in DT can also benefit from this study to optimise their resource allocation (Müller et al., 2015). Furthermore, the study can enhance supply chain security, a facet of DT frequently disregarded (Taylor et al., 2020).

Understanding user behaviour and potential security risks is critical, as humans are vital to DT security. Therefore, this research identifies guidelines for developing training and awareness initiatives that educate stakeholders and employees about cybersecurity issues (e.g., D'Arcy et al., 2009; Schneier, 2011; Crossler et al., 2013).

Regardless of how matured an organisation believes its cyber threat intelligence is, this research can help gather and disseminate threat intelligence and inform organisations about the latest threats and vulnerabilities. Such timely defence depends on this type of intelligence-collected data. Given the holistic role of NFC, experts from different fields can work together across disciplines to address the complex challenges of DT (Winniford, 2009; Barlette & Fomin, 2008; Lowry et al., 2017).

Ultimately, this research has the potential to influence cybersecurity policy and legislation. It can provide policymakers and regulators with fact-based guidance to ensure a secure digital environment. The NFC cybersecurity model can potentially have a significant global impact as the issues raised by the digital revolution are not restricted to a solitary field or economic sector. This research has implications for a vast, interconnected digital world (Goel & Chengalur, 2010; Baskerville & Siponen, 2002).

In conclusion, exploring cybersecurity issues in digital transformation is critical to strengthening organisational resilience and protection against shifting cyber threats and the accelerating digitalisation of organisation operations. The NFC cybersecurity model can help organisations make intelligent decisions and align with the changing cybersecurity ecosystem.

1.6. Structure of Thesis

This section outlines the systematic development of this study, presenting six contributions to the cybersecurity of IS and the key initiatives organisations face. The contributions are listed and summarised below.

Papers addressing the adoption of digital products and services such as financial technology (FinTech) and cloud computing, e.g., Infrastructure as a Service (IaaS):

Stewart, H., and Jürjens, J. (2018), "Data security and consumer trust in FinTech innovation in Germany", *Information & Computer Security*, vol. 26, no. 1, pp. 109–128.

<https://doi.org/10.1108/ICS-06-2017-0039>.

Stewart, H. (2021), "The hindrance of cloud computing acceptance within the financial sectors in Germany", *Information and Computer Security*, Vol. ahead-of-print No. ahead-of-print.

<https://doi.org/10.1108/ICS-01-2021-0002>.

Paper addresses cybersecurity strategy and compliance with industry standards to improve DT cybersecurity:

Stewart, H. (2022), "Security versus Compliance: An Empirical Study of the Impact of Industry Standards Compliance on Application Security ", *International Journal of Software Engineering and Knowledge Engineering*, Vol. 32. <https://doi.org/10.1142/S021819402250015>.

Papers focusing on data protection, information protection and cybersecurity investment decisions:

Stewart, H. (2022) 'Digital Transformation Security Challenges, *Journal of Computer Information Systems*, DOI: 10.1080/08874417.2022.2115953

Stewart, H., and Jürjens, J. (2017), "Information security management and the human aspect in organisations", *Information & Computer Security*, vol. 25, no. 5, pp. 494–534.

<https://doi.org/10.1108/ICS-07-2016-0054>.

Stewart, H. (2022), "A systematic framework to explore the determinants of information security policy development and outcomes", *Information and Computer Security*, Vol. ahead-of-print No. ahead-of-print. <https://doi.org/10.1108/ICS-06-2021-0076>

An overview of each paper's content and relevance to the research objectives is summarised below:

Paper 1: Data security and consumer trust in FinTech innovation

Paper 1 analyses the decision-making processes of managers and consumers when adopting new disruptive technologies. Ensuring the security of financial data and gaining consumer trust are crucial factors in the fast-paced development of FinTech innovation. As the FinTech industry continues transforming the financial landscape, ensuring the security of sensitive financial data, and building consumer trust are crucial for success (Carlson, 2015). The paper focuses on the misconceptions of managers and consumers about DT, drawing on prospect theory and previous research (Carlson, 2015) and examines the impact of DT on the decision-making processes of managers and consumers. This research proposes a model called "Intention to adopt FinTech", where the constructs were developed based on the Technology Acceptance Model (TAM) (Straub et al., 1997) and five additional components

such as customer trust, data security, added value, user interface design and FinTech promotion (Stewart & Jürjens, 2018). A dataset of 209 customers was collected through an online survey and face-to-face interviews to test this model. The empirical results show that attitudes towards DT or new technologies adoption strongly depend on data security, customer trust and user interface (Duc & Chirumamilla, 2019; Ande et al., 2020).

To summarise, the connection between data security and consumer trust plays a crucial role in the prosperity and sustainability of FinTech innovation (Duc & Chirumamilla, 2019). As the industry grows, FinTech companies must manoeuvre through the intricate terrain of compliance, data security, and user trust to establish and retain their competitive edge (Eder-Neuhauser et al., 2018; Bullée & Junger, 2020; Hadnagy, 2018). Sustaining customer trust necessitates keeping lines of communication open and taking proactive measures, as security, customer trust, and data breaches can have grave consequences (Duc & Chirumamilla, 2019). This paper answers the first research question regarding how consumers and employees perceive DT.

Paper 2: The hindrance of cloud computing acceptance within the financial sectors

Paper 2 builds upon Paper 1 by providing a comprehensive analysis of the identified constraints. This research paper addresses managers' concerns about the security of cloud migration in other words, Infrastructure as a service (IaaS). It draws on previous studies such as Modi et al. (2012), Coppolino et al. (2016) and Sharma and Trivedi (2014) that examine the security challenges of cloud computing. This paper develops a research model called "IaaS Adoption" based on the NFC model (Oliveira et al., 2014), which includes the TAM (Straub et al., 1997), trust, data security and risk (Stewart & Jürjens, 2018) as main components to assess the perceived adoption of cloud computing (Belbergui, 2017) and the associated benefits and risks (Babak et al., 2015). This model is empirically tested based on a data set of 208 bank employees gathered via an online survey. Based on the results, managers' views on new technologies, specifically IaaS, are influenced by their perception of the benefits and risks of their current technology and their prior experience with the new technology (Lee, 2012). The extent of IaaS usage in their industry determines this experience. The assessment of their current technology significantly impacts managers' misinterpretation of IaaS. As a result, they may overestimate the risks associated with IaaS (Al-Khater et al., 2020), leading to a preference for the legacy system. Prospect theory declares this as loss-aversion theory, which can hinder the adoption of a potentially advantageous new technology (Kahneman & Tversky, 1979).

The financial industry is adopting cutting-edge security measures, tightening regulatory requirements for the cloud and leveraging multiple hybrid or multi-cloud approaches for greater flexibility and control to overcome these obstacles (Trivedi, 2014). The financial sector is becoming more receptive to the potential of cloud computing (Babak et al., 2015) as cloud providers improve their security, compliance and privacy features (Trivedi, 2014). It is critical to take proactive measures and maintain transparent communication to maintain customer trust, as data breaches and security incidents can have serious consequences (Al-Khater et al., 2020). This paper answers the second research question regarding cybersecurity vulnerabilities associated with cloud computing and the factors that hinder its adoption.

Paper 3: Security versus compliance: an empirical study of the impact of industry standards compliance on application security

This paper explores the connection between the level of compliance with industry standards and the actual security level of applications. Through empirical research, this study delves into the complex relationship between adherence to established standards and the effectiveness of security measures in application development (Sahu, 2019; Stewart, 2022; Calero, 2013). Organisations face a continuous challenge in balancing regulatory compliance with application security (Calero, 2013). Often, organisations invest a large amount of resources into meeting regulations but overlook security vulnerabilities (Stallings et al., 2012). This study sheds light on this and examines the impact of industry-specific compliance requirements such as ISO27001, PCI DSS, and HIPAA on the security of applications and whether compliance measures lead to better security procedures.

In today's fast-paced world, businesses must adopt the latest technologies and software applications to streamline their work processes. This process of DT involves replacing outdated tools with cutting-edge solutions. While efforts are being made to enhance application security and prevent unauthorised access to critical applications, practical challenges remain. Several studies have been conducted on this topic, including those by Stewart (2020), Sahu (2019), Calero (2013), Sahu et al. (2014), and Kumar (2015).

Despite the recommendations of security experts to implement regulatory standards like ISO27001, NIST, and PCI, cyber threats to applications persist (Stallings et al., 2012). If a company's digital products and services are secure, individuals may be more inclined to adopt new technologies than if they are compliant with industry standards. While the focus of cybersecurity is on mitigating business risks, the focus of compliance is on regulatory requirements (Hassan et al., 2015). Both cybersecurity and

industry standards aim to manage risks and protect sensitive data and systems, but they follow different processes and workflows to achieve these goals. Given the increasing amount of data and the associated security risks, protecting data is a major concern for organisations and individuals (Karjalainen, 2019). In addition to technical measures such as secure coding and the implementation of secure APIs, typical data protection measures such as password authentication revolve around end users, often referred to as the weakest link in the information security chain (Flowerday, 2016).

This paper uses both qualitative and quantitative methods to analyse the vulnerabilities of different content relationship management (CRM) systems used by two organisations: One group adheres to a regulatory standard, and the other does not. Six hackers conducted penetration testing on both CRM systems before and after the research. Semi-structured interviews were conducted to understand developers' views on application security compliance and regulatory standards, including their current practices and ability to follow application security policies. The data collected showed that cybersecurity is more significant in ensuring a secure DT than organisations relying solely on industry standards like ISO27001. The study also found that organisations that adopt an industry standard can improve their security by implementing a cybersecurity strategy, which is crucial for developing secure digital products and services (Kumar et al., 2019).

The empirical study highlights the importance of a balanced approach to application security and compliance with industry standards. While compliance is essential, organisations must recognize its limitations and implement a more comprehensive, proactive security approach to safeguard their applications against dynamic, constantly changing security threats (Karpunina et al., 2019). This study emphasises that a comprehensive strategy combining compliance with solid security measures is required to handle the current threat landscape's complexity properly. This paper answers the third research question related to the impact of cybersecurity strategy during software development in organisations that adhere to an industry standard such as ISO27001 (Soomro et al., 2016).

Paper 4: DT Security Challenges

Paper 4 builds upon Papers 1, 2, and 3 by delving deeper into previously identified obstacles. The study examined 39 pieces of research on information security in the public and private sectors, as well as by individuals in these fields. Its objective was to understand why digital security and information systems security remain significant concerns for most organisations and individual users of modern technology, as seen in the case studies presented in previous papers.

In spite of the many advantages that DT offers, it also presents several security challenges that organisations must tackle (Ramachandran, 2015; Djemame, 2016). These challenges stem from incorporating innovative technologies, increased connectivity, and the constantly changing threat landscape (Armbrust et al., 2010). Compliance with laws and standards such as GDPR, HIPAA, or industry-specific requirements (Soomro et al., 2016) can be complicated due to DT's frequent crossing of international borders (Armbrust et al., 2010). The shift to the cloud introduces new security risks, and cloud-based data storage requires strong access controls, encryption, and protection against data breaches (Modi, 2012).

This research proposes a framework called “Digital Security Strategy (DSS)”, in which eight constructs have been developed based on the findings of numerous research papers; misperceptions about security, vulnerability and risk assessments, cybersecurity strategy, secure systems engineering, testing and evaluation, protective monitoring, strategic advanced threat intelligence, incident response, and remediation are all critical components of DT but are often un(der)developed in DT (Al-shqeerat et al., 2017, Nada et al., 2017).

An integrated approach is needed to address the challenges of security (Nada et al., 2017).

Organisations should take proactive measures, leverage robust security technologies, and embed security at the core of their DT strategies (Oliveira et al., 2014). Collaboration between IT, security and compliance teams is critical to minimise risks and protect digital initiatives (Shahri & Mohanna, 2016; Singh & Hess, 2017).

The study offers context-specific insights into how the identified obstacles affect different stakeholders, including researchers, small and medium-sized enterprises, large enterprises, and governments. This paper answers the fourth research question on the main challenges of DT and provides solutions to overcome them.

Paper 5: Information security management and the human aspect in organisations

In Paper 5, the results of previous research are combined to develop a new cybersecurity model called the Nine-Five Circle (NFC) for decision-making in cybersecurity improvement, focusing on information security management system (ISMS) (Maynard et al., 2011; Khansa & Liginlal, 2007) and ISP (Sahu, 2019; Stewart, 2022; Calero, 2013). The model considers contextual aspects such as the role of humans in information security (Kraemer et al., 2009), the financial impact of information security, the misuse of information security knowledge (Kusserow, 2014), cybersecurity intelligence maturity, the role of

technology in information security, and industry standards for information security management (Shahri & Mohanna, 2016; Singh & Hess, 2017). The data collected from 233 expert interviews is analysed using the structural equation model (SEM) as in the work of Hair et al. (2010).

The NFC model draws on previous research on organisational DT security and highlights that most decisions are based on statistical theories (Singh & Kaul, 2016; Siponen & Willison, 2009; Siponen et al., 2014). However, this paper suggests that more research is needed on decision-making from the behavioural, environmental, and organisational perspectives of managers and employees, with a focus on an effective ISP (Stahl et al., 2012), which is an important mechanism to combat insider threats (Siponen et al., 2014). The paper concludes that considering these factors is crucial to making informed decisions about DT in the future and answers the research question five.

Effective information security management in organisations requires a strong focus on the human element. This means considering human behaviour (Siponen et al., 2014), promoting security awareness, cultivating a culture of security consciousness and establishing guidelines and procedures involving employees in protecting sensitive information (Maynard et al., 2011). A holistic approach that combines technology- and human-centred strategies is the key to effectively mitigating security risks.

Paper 6: A systematic framework to explore the determinants of information security policy development and outcomes:

In Paper 6, the impact of contextual aspects on organisational ISP and compliance is explored further, building on the NFC model (Thakare et al., 2020). A systematic framework that examines the factors that influence the development and outcomes of ISPs to ensure the effective development and implementation of ISPs in organisations. This framework should help identify the key variables that impact policy development and assess their impact on security outcomes.

This research aims to create an organisational model that outlines modern organisations' comprehensive security policy process (Sohrabi et al., 2016). Despite extensive research, less models have been found in academic or practice-based literature (Bragg, 2002; Thakare et al., 2020). The proposed model is based on recommended practices from certified information security professionals and reflects an information security policy process (Negreiro & Madiega, 2019).

Qualitative techniques were employed to develop the NFC model, identifying primary policy processes, key environmental and organisational influences, and their underlying linkages. This chapter delves into organisational leadership's important role and responsibility in recognising the need for ISPs (Sohrabi et

al., 2016), particularly in today's rapidly evolving security landscape (Forrester Research, 2018). It covers DT ISPs that apply to all security models and practices and the complexities of developing and implementing them (Finjan Team, 2019). ISP helps identify and evaluate risk levels using available technological security tools and lays out management strategies for crafting effective policies and selecting appropriate public notice (Hemerlin et al., 2018).

It is found that research in organisational ISP has neglected the holistic approach required to develop a successful ISP and compliance (Paananen et al., 2020). Additionally, certain theoretical assumptions are not necessarily applicable in the context of DT. Through a literature review and conceptualization of general characteristics of DT, various constraints are validated, such as security intelligence, cyber threat intelligence, external partners, organisational commitment, information security misperception, and information security investment (Lucila, 2016; Tuyikeze & Flowerday, 2014; Maynard & Ruighaver, 2006). These constraints are contextualised in terms of their influence on ISP through 30 expert interviews. The findings suggest that several widely held assumptions in the existing ISP literature should be changed if researchers claim generalizability of their findings in a DT context (Lucila, 2016). Exemplary assumptions include the planning, formalisation, documentation, development, and adherence to information security policies (Bulgurcu et al., 2010), often non-existent or underdeveloped in DT.

In addition, this study provides recommendations for future research on the impact of identified constraints on decision-making in organisations undergoing DT. Specifically, it suggests applying the framework to cases of failure. Organisations must ensure that their policies are enforced and compliant through regular reviews (Thakare et al., 2020). This paper answers the sixth research question on ISP determinants and outcomes.

A systematic framework can facilitate researchers and organisations in understanding the factors that impact ISP development and security outcomes.

1.7. References

- A. Fielder, E. Panaousis, P. Malacaria, C. Hankin and F. Smeraldi, "Decision support approaches for cyber security investment", *Decision Support Syst.*, vol. 86, pp. 13-23, Jun. 2016.
- Abir M'baya, Jannik Laval, Nejib Moalla, "An assessment conceptual framework for the modernization of legacy systems", 2017 11th International Conference on Software, Knowledge, Information Management and Applications (SKIMA), pp.1-11, 2017.
- Agrawal, Divyakant, Amr El Abbadi, and Shiyuan Wang (2013) "Secure and privacy-preserving database services in the cloud," in *The 29th International Conference on Data Engineering (ICDE)*, IEEE.
- Al-Kaabi, Reem (2010) "Critical success factors of e-government: A proposal model for e-government implementation in Kingdom of Bahrain," in *Proceeding of the 6th International Conference one-Government (ICEG)*.
- Alvesson, M., & Sandberg, J. (2011). *Generating Research Questions through Problematization*. *Academy of Management Review*, 36(2), 247–271
- Ande, R., Adebisi, B., Hammoudeh, M., Saleem, J. (2020), "Internet of Things: Evolution and technologies from a security perspective", *Sustainable Cities and Society* 54, 101728. <https://doi.org/10.1016/j.scs.2019.101728>.

- Arbanas, K., & Hrustek, N. Ž. (2019), "Key Success Factors of Information Systems Security", *Journal of Information and Organisational Sciences*, 43(3), 131-144.
- Arendt, L. (2008). Barriers to ICT Adoption in SMEs: How to Bridge the Digital Divide? *Journal of Systems and Information Technology*, 10(2), 93–108.
- Bakar, H.A.; Razali, R.; Jamari, D.I. Legacy Systems Modernisation for Citizen-Centric Digital Government: A Conceptual Model. *Sustainability* 2021, 13, 13112. [CrossRef]
- Baker, W. H., Rees, L. P., & Tippett, P. S. (2007). Necessary Measures—Metric-drive Information Security Risk Assessment and Decision-Making. *Communications of th ACM*, 50(10), 101–106.
- Beaudin, K. College and university data breaches: Regulating higher education cybersecurity under state and federal law. *J. Coll. Univ. Law* 2015, 41, 657–693.
- Bongiovanni, I. The least secure places in the universe? A systematic literature review on information security management in higher education. *Comput. Secur.* 2019, 86, 350–357.
- Bragg, R. (2002). Policies, Standards, Guidelines, and Procedures. *CISSP Security Management and Practices Training Guide*.
- Bullée, J. W., Junger, M. (2020). "Social Engineering". 10.1007/978-3-319-90307-1_38-1.
- Burns, N. & Grove, S. K. (2001), "The practice of nursing research: Conduct, critique, and utilization". Philadelphia, PA: Saunders.
- Chapman, J. How Safe Is Your Data? Cyber-Security in Higher Education. HEPI Policy Note, April 2019.
- Collet. S (2020), "What is security's role in digital transformation?" <https://www.csoonline.com/article/3512578/what-is-securitys-role-in-digital-transformation.html>, 2020. [Online; accessed 23-September-2022].
- Cragg, P., Caldeira, M., & Ward, J. (2011). Organizational Information Systems Competences in Small and Medium-sized Enterprises. *Information & Management*, 48(8), 353–363.
- Duc, A.N & Chirumamilla, A (2019). "Identifying Security Risks of Digital Transformation ", *An Engineering Perspective*. 677-688. 10.1007/978-3-030-29374-1_55.

- Eder-Neuhauser, P., Zseby, T., Fabini, J. (2018), "Malware propagation in smart grid monocultures
Malware-Ausbreitung in Smart Grid-Monokulturen", *Elektrotechnik and Informationstechnik*
135 (3), 264–269.
- Eurostat. (2015). Statistics on Small and Medium-sized Enterprises—Dependent and Independent SMEs
and Large
Enterprises. http://ec.europa.eu/eurostat/statistics-explained/index.php/Statistics_on_small_and_medium-sized_enterprises. Accessed 19 Feb 2022
- Finjan Team. (2019). What is Digital Transformations Impact on Cyber Security? Finjan Cybersecurity –
Finjan Blog. <https://blog.finjan.com/what-is-digital-transformations-impact-on-cybersecurity/>
- FireEye, Inc. Why Cyber Attackers Are Targeting Higher Education, and What Universities Can Do about
It. White Paper. Library Catalog, 2015. Available online: www.fireeye.com (accessed on 28
January 2021).
- Foerster-Metz, Ulrike Stefanie, Katrin Marquardt, Nina Golowko, Andreas Kompalla, and Christian Hell.
(2018) "Digital transformation and its implications on organisational behavior," *Journal of EU
Research in Business* 2018 (3): 1-14.
- Hemerling, J., Kilmann, J., Danoesastro, M., Stutts, L., & Ahern, C. (2018). It's not a digital
transformation without a digital culture. Boston Consulting Group.
- Holweg, Matthias & boer, harry & Schmenner, Roger & Pagell, Mark & Kilduff, Martin & Voss, Chris.
(2015). Making a meaningful contribution to theory. *International Journal of Operations &
Production Management*. 10.1108/IJOPM-03-2015-0119.
- Ifinedo, Princely (2014) "Information systems security policy compliance: An empirical study of the
effects of socialisation, influence, and cognition," *Information & Management* 51 (1): 69–79
- Imgrund, Florian, Marcus Fischer, Christian Janiesch, and Axel Winkelmann (2018) "Approaching
digitalisation with business process management," in *Proceedings of the MKWI*
- Introna, L. D. & Wood, D. (2004), "Picturing algorithmic surveillance: The politics of facial recognition
systems". *Surveillance & Society*, 2, 177-198.

- Jonathan, Gideon M. (2019) "Digital transformation in the public sector: Identifying critical success factors," in European, Mediterranean, and Middle Eastern Conference on Information Systems, Springer.
- Julian A. García-García, C. Arevalo Maldonado, Ayman Meidan, Esteban Morillo-Baro, María José Escalona, "gPROFIT: A Tool to Assist the Automatic Extraction of Business Knowledge From Legacy Information Systems", *IEEE Access*, vol.9, pp.94934-94952, 2021.
- Karpunina, E.K., Konovalova, M.E., Shurchkova, Julia, V.S., Isaeva, Ekaterina, A., and Abalakin, A.A. (2019), "Economic security of businesses as the determinant of digital transformation strategy", In Institute of Scientific Communications Conference, pages 251–260. Springer.
- Karumbaiah, S., Wright, R.T., Durcikova, A., Jensen, M. L. (2016), "Phishing training: A preliminary look at the effects of different types of training", In Proceedings of the 11th Pre-ICIS Workshop on Information Security and Privacy, pages 1–10.
- Karyda, M. Kiountouzis, E., and Kokolakis, S. (2005), "Information Systems Security Policies: A Contextual Perspective," *Computers & Security* (24:3), pp 246-260.
- Khan, M.; Ali, I.; Nisar, W.; Saleem, M.Q.; Ahmed, A.S.; Elamin, H.E.; Mehmood, W.; Shafiq, M. Modernization Framework to Enhance the Security of Legacy Information Systems. *Intell. Autom. Soft Comput.* 2022, 32, 543–555. [CrossRef]
- Kranz, M., Murmann, L., & Michahelles, F. (2013), "Research in the large: Challenges for large-scale mobile application research: A case study about NFC adoption using gamification via an app store". *IJMHCI*5(1), 45-61. doi:10.4018/jmhci.2013010103.
- Kwon, J., & Johnson, M. E. (2014). Proactive Versus Reactive Security Investments in the Healthcare Sector. *Management Information Systems Quarterly*, 38(2), 451–471.
- Lundgren, B., & Möller, N. (2017). Defining Information Security. *Science and Engineering Ethics*, 25(3), 1-8.
- Luse, A., Mennecke, B., Townsend, A., Demarie, S. (2013), "Strategic Information Systems Security: Definition and Theoretical Model," *AMCIS 2013*, August 15-17. Chicago, USA.
- Luse, A., Mennecke, B., Townsend, A., Demarie, S. (2013), "Strategic Information Systems Security: Definition and Theoretical Model," *AMCIS 2013*, August 15-17. Chicago, USA.

- M. Kazemi, "Evaluation of information security management system success factors: Case study of municipal organization", *Afr. J. Bus. Manage.*, vol. 6, no. 14, pp. 4982-4989, Apr. 2012.
- Maleks Smith, Z., E. Lostri, and J.A. Lewis. 2020. The hidden costs of cybercrime.
<https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf>.
Accessed 10 October 2023.
- Matt, Christian, Thomas Hess, and Alexander Benlian (2015) "Digital transformation strategies." *Business & Information Systems Engineering* 57 (5): 339– 343.
- Mitnick, K. & Simon, W. L. (2002), "The art of deception: Controlling the human element of security", New York, NY: John Wiley & Sons.
- Möller, A., Michahelles, F., Diewald, S., Roalter, L., & Kranz, M. (2012), "U Kranz pdate behaviour in app markets and security implications: A case study in Google play", In: Poppinga B. (ed.), *Proceedings of the 3rd International Workshop on Research in the Large, held in Conjunction with Mobile HCI*, pp. 3-6.
- Moon, Yun Ji, Myeonggil Choi, and Deborah J. Armstrong. (2018) "The impact of relational leadership and social alignment on information security system effectiveness in Korean governmental organisations." *International Journal of Information Management* 40 : 54-66.
- Muehe, S., & Drechsler, A. (2017). Towards a Framework to Improve IT Security and IT Risk Management in Small and Medium Enterprises. *International Journal of Systems and Society*, 3(2), 44–56
- Myers, M. D. (1997). *Qualitative Research in Information Systems*. *MIS Quarterly*, 21(2),
- Nazareth, D. L., & Choi, J. (2015). A System Dynamics Model for Information Security Management. *Information & Management*, 52(1), 123–134.
- Negreiro, M., Madiega, T. (2019). *Digital Transformations. Briefing – EU Policies – Delivering for Citizens*. European Parliament Research Services. Members' Research Service PE 633.171.
- Oliveira,T., Thomas, M., Espadanal, M. (2014), "Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors". *Journal of Information & Management*, 51, pp.497–510.

- Qian, Y., Fang, Y., & Gonzalez, J. J. (2012). Managing Information Security Risks During New Technology Adoption. *Computers & Security*, 31(8), 859–869.
- Rees, L. P., Deane, J. K., Rakes, T. R., & Baker, W. H. (2011). Decision Support for Cybersecurity Risk Planning. *Decision Support Systems*, 51(3), 493–505.
- Samonas, S., Coss, D. (2014), "The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security", *Journal of Information System Security* 10 (3), 21–45.
- Sausalito, C. (2020), "Cybercrime To Cost The World \$10.5 Trillion Annually By 2025. New York", *Cybercrimme Magazine*.
- Schatz, D., & Bashroush, R. (2017). Economic Valuation for Information Security Investment: A Systematic Literature Review. *Information Systems Frontiers*, 19(5), 1205–1228.
- Shahri, A. B., & Mohanna, S. (2016), "The Impact of the Security Competency on "Self-efficacy in Information Security" for Effective Health Information Security in Iran", *The Advances in Intelligent Systems and Computing*, 445, 51-65.
- Sheehan B, Murphy F, Mullins M, Ryan C. Connected and autonomous vehicles: A cyber-risk classification framework. *Transportation Research Part a: Policy and Practice*. 2019;124:523–536. doi: 10.1016/j.tra.2018.06.033.
- Siponen, M. (2005). An Analysis of the Traditional IS Security Approaches: Implications for Research and Practice. *European Journal of Information Systems*, 14(3), 303–315.
- Sonnenschein, R., Loske, A., & Buxmann, P. (2017). The Role of Top Managers' IT Security Awareness in Organizational IT Security Management. *Proceedings of the 38th International Conference on Information Systems*, South Korea.
- Soomro, Zahoor Ahmed, Mahmood Hussain Shah, and Javed Ahmed (2016) "Information security management needs more holistic approach: A literature review," *International Journal of Information Management* 36 (2): 215–225.
- Stewart, H., and Jürjens, J. (2017), "Information security management and the human aspect in organisations", *Information & Computer Security*, vol. 25, no. 5, pp. 494–534. <https://doi.org/10.1108/ICS-07-2016-0054>.

- Stewart, H., and Jürjens, J. (2018), "Data security and consumer trust in FinTech innovation in Germany", *Information & Computer Security*, vol. 26, no. 1, pp. 109–128.
<https://doi.org/10.1108/ICS-06-2017-0039>.
- Stewart, H. (2022), "A systematic framework to explore the determinants of information security policy development and outcomes", *Information and Computer Security*, Vol. ahead-of-print No. ahead-of-print. <https://doi.org/10.1108/ICS-06-2021-0076>
- Thakare, Vaishali & Bhushan S, Bharath & Goundar, Sam. (2020). *Impact of Digital Transformation on Security Policies and Standards*. 10.4018/978-1-7998-2367-4.
- Thorwat, S. R. (2018), "ICT in Higher Education: Opportunities of Urban Colleges and Challenges of Tribal Colleges", *International Research Journal of Multidisciplinary Studies*, 1-6.
- Tom Tervoort, Marcela Tuler De Oliveira, Wolter Pieters, Pieter Van Gelder, Silvia Delgado , Henk Marquering, "Solutions for Mitigating Cybersecurity Risks Caused by Legacy Software in Medical Devices: A Scoping Review", *IEEE Access*, vol.8, pp.84352-84361, 2020.
- Tu, Cindy Zhiling, Yufei Yuan, Norm Archer, and Catherine E. Connelly. (2018) "Strategic value alignment for information security management: A critical success factor analysis," *Information & Computer Security* 26 (2): 150-170.
- Unit-Department for ICT and Joint Services in Higher Education and Research. Technical Report. 2019. Available online:
https://www.regjeringen.no/contentassets/f464322e9623456dabe220571dfab8f6/unit-okonomiseminar_2019.pdf (accessed on 10 October 2023).
- Vial, Gregory (2019) "Understanding digital transformation: A review and a research agenda," *The Journal of Strategic Information Systems* 28 (2): 118–144.
- W. A. Conklin, R. E. Cline and T. Roosa, "Re-engineering cybersecurity education in the U.S.: An analysis of the critical factors", *Proc. 47th Hawaii Int. Conf. Syst. Sci.*, pp. 2006-2014, Jan. 2014.
- Wang, J., Chaudhury, A., & Rao, H. R. (2008). A Value-at-Risk Approach to Information Security Investment. *Information Systems Research*, 19(1), 106–120.
- Wang, T., Kannan, K. N., & Rees Ulmer, J. (2013). The Association Between the Disclosure and the Realization of Information Security Risk Factors. *Information Systems Research*, 24(2), 201–218.

- Wangen, G. Quantifying and Analyzing Information Security Risk from Incident Data; Graphical Models for Security; Albanese, M., Horne, R., Probst, C.W., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 129–154.
- Weishäupl, E., Yasasin, E., & Schryen, G. (2015). A Multi-Theoretical Literature Review on Information Security Investments using the Resource-Based View and the Organizational Learning Theory. Proceedings of the 36th International Conference on Information Systems (ICIS), Fort Worth, USA
- Yang, C. G., & Lee, H. J. (2016). A Study on the Antecedents of Healthcare Informatio Protection Intention. *Information Systems Frontiers*, 18(2), 253–263.
- Yeniman, Y., Ebru Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing information security management in small-and medium-sized enterprises: a case study from turkey. *International Journal of Information Management*, 31(4), 360–365.
- Yildirim, E., Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing Information Security Management in Small-and Medium-sized Enterprises: A Case Study from Turkey. *International Journal of Information Management*, 31(4), 360–365.
- Yilmaz, R.; Yalman, Y. A Comparative Analysis of University Information Systems within the Scope of the Information Security Risks. *TEM J.* 2016, 5, 180–191.

Chapter 2. Literature Review (Theoretical Background)

This section provides an overview of the theoretical foundations and complements the theoretical background of the six individual papers. The first part explains the concept of DT, while the second part deals with cyber security and industry standards. The last section briefly discusses information security policy in IS research.

This section presents the theoretical foundations of IS research and six published papers. Various DT concepts are introduced to help readers understand the topic. The goal is to clarify and provide context for DT challenges. Each paper uses this foundation as a framework for this thesis. The papers also explore ways to enhance cybersecurity in DT. The six papers aim to propose a theoretical concept of DT cybersecurity and create a descriptive cybersecurity model from a global perspective.

To ensure the reliability of a research project, it is essential to conduct a comprehensive analysis of current scientific practices, also referred to as state-of-the-art analysis. To address the research questions posed in this thesis, it is vital to examine the use of scientific theories and research methods. Correctly understanding this requires explaining how the thesis reflects the scientific view. The scientific approach and methods used depend on the specific problems and questions studied. Therefore, this chapter draws from the six published papers that are the primary focus of the research:

1. DT Challenges
2. Financial Technology adoption challenges
3. Cloud computing adoption challenges
4. Security versus Industrial Standards
5. Information security management system
6. Information security policy and compliance

2.1. Digital Transformation

Prior to the term being coined, Dougherty discussed the concept of digitalisation, which refers to the transition from analogue to digital technology. Dougherty also foresees the emergence of ubiquitous computing and its impact on the way humans and organisation's function (Gartner, 2019).

Morakanyane and colleagues (2017) conducted a thorough literature review and defined "DT" as a process that utilises digital capabilities and technologies to enhance business models, operational processes, and customer experiences to create value (p. 437). As a result, enabling DT is an essential goal for leaders worldwide (Hess et al., 2016). According to Stewart's (2021) research, modern technologies significantly impact all aspects of a business and its ability to create value for customers. Additional studies suggest that organisations can only thrive in today's digital age if they adopt DT (Stewart & Jürjens, 2018; Urbach & Röglinger, 2018).

Past DT studies have focused on two distinct but related theoretical perspectives. Within the first approach, DT involves utilising digital technologies to substantially advance an organisation's operations or scope by empowering changes in organisational patterns, behaviours, and cultures (Bekkhus, 2016; Bharadwaj et al., 2013; Matt et al., 2015). Thus, the integration of IT strategy into organisational business strategy has moved beyond the operational level (Bharadwaj et al., 2013). The second strategy, justified by the notion that DT extends beyond IT implementation, emphasises merging structural change with digital technology to forge new value-generation channels (Hess et al., 2016). According to Wessel et al. (2020), DT programmes should strengthen a company's value proposition through digital technology and reinvention.

To succeed in DT, companies need a strategy that is aligned with their goals and considers the impact of technology on processes and offerings. Consequently, managers and decision-makers need to determine how to balance technology use, value creation, structural change, and fiscal impact. In this context, the decision to adopt a particular technology may not only be based on investment and profitability, but also has process implications and can reshape a company's product and service portfolio in addition to its value proposition in general (e.g., Stewart & Jürjens, 2018; Urbach & Röglinger, 2018).

Studies show that managers and researchers face challenges in deciding which DT skills and technologies to invest in and how to perceive them (e.g., Gomber et al., 2018; Stewart & Jürjens, 2018). For instance, a large body of theory-based justifications for technological changes in the financial

services sector is provided in the IS literature (e.g., Stewart & Jürjens, 2018; Han et al., 2008; Clemons et al., 1996; Goh et al., 2013). DT has changed the modern business landscape across industries (Meraviglia, 2018) and created opportunities for innovative start-ups to deliver customer value (Stewart & Jürjens, 2018; Rogers, 2016). There are many ethical, legal, and organisational factors to consider when considering whether to invest in and adopt a new technology. These include ensuring security and privacy, complying with regulations and laws, and assessing potential risks and vulnerabilities. Financial Technology (FinTech) and cloud computing are prime examples of a technology where all these aspects need to be considered (e.g., Modi et al., 2012; Coppolino et al., 2016; Ramachandran, 2015; Stewart & Jürjens, 2018; Stewart, 2021) with most start-ups focusing more on speed and functionality and neglecting the security aspect of maintaining data confidentiality, integrity, and availability (Ellström et al., 2022; Warner & Wäger, 2019). The provision of cybersecurity amid DT offers tremendous storage and processing capabilities, making it an essential tool for DT. Cybersecurity protects internet-connected devices and services from attacks by hackers, spammers, and cybercriminals. It prevents phishing schemes, ransomware attacks, identity theft, data breaches, and financial losses.

Due to the complexity of cyber issues, companies are often reluctant to invest in large-scale DT efforts that require more resources (Kane et al., 2019; Hess et al., 2016). Additionally, the vulnerability resulting from integrating various systems increases the cyber threat. The lack of a firm cybersecurity strategy and the misperception of cybersecurity by stakeholders pose a challenge to DT, as DT requires coherent efforts (Maedche, 2016). The security challenges need to be addressed to tackle DT. Although DT tends to harness and foster more creativity through the information and computing capabilities that enable novel forms of collaboration between networked actors, this creativity also heightens security-related threats, particularly the increase in human-technology interactions and security threats in social networks.

Researchers have studied the security challenges of DT from different theoretical perspectives, and numerous proposals have been made over the decades, ranging from cybersecurity models to industrial cybersecurity frameworks. The most applied industrial framework models include the ISO27K family and the NIST CF, widely used as a unified approach to DT protection (Ellström et al., 2022; Warner & Wäger, 2019). The foundation of these frameworks is a hierarchy of capabilities, including risk assessment, information security policy (ISP) development, compliance, data protection, employee behaviour and cybersecurity (Tece, 2018). All these capabilities are linked to DT as they help

organisations devise secure strategies to improve their current business models and develop new ones while managing current and future risks (Warner & Wäger, 2019).

An organisation's DT depends on cybersecurity maturity and flexibility, which can be achieved through three dynamic capabilities: leadership, culture, and change. These three dynamics ensure leadership support for cybersecurity initiatives and the identification of opportunities and risks. Culture provides the integration of cybersecurity into the organisational culture (Hu et al., 2012), and change is the organisation's willingness to change and adopt cybersecurity training.

The argument presented in this section is that while DT requires continuous adaptation and the use of cutting-edge technologies to improve the customer experience and deliver value to organisations (Newitt, 1996; von Leipzig et al., 2017; Vial, 2019), cybersecurity issues are a significant barrier to achieving economic scale for many organisations and need to be addressed through a comprehensive cybersecurity solution. Financial technology and cloud computing are two prominent examples of cutting-edge technology that embody the aforementioned considerations. Cloud computing is often referred to as one of the key enablers of DT, facilitating the sharing and processing of data on a large scale. The evolution of financial technology and data storage and processing via cloud computing are discussed in more detail in the following sections.

2.2. Financial Technology (FinTech)

The banking sector has undergone a major financial revolution with the introduction of the Internet of Things. In the past, telegraphs were used for financial transactions as early as 1838. However, the banking industry has since utilised information technology to streamline operations (Eyal, 2017). The Internet has brought about technological innovation in various fields, including the emergence of FinTech, an innovative financial business that uses technology to enhance financial transactions (Schueffel, 2016). FinTech refers to contemporary financial interactions, especially those related to internet technology, such as mobile Internet and cloud computing, and operational processes in the financial services sector, such as banking and monetization. FinTech is disrupting the financial industry through automated processes and the availability of information and communication technology (ICT). FinTech offers various business models in the financial services industry that combine security, pace, and innovation (Casoria, 2018). International organisations and global standard setters, led by Casoria in 2018, have created a modern conceptual model known as the FinTech Tree. The model categorises FinTech into three categories: FinTech activities, enabling technologies, and policy enablers. These activities take place in diverse finance sectors and formats.

Despite the substantial amount of research examining the process and techniques employed to effectively accept the adoption of FinTech, there is still the absence of a complete model to depict the disruptive FinTech innovation process in terms of data security and trust. Current innovation adoption theories and models must be modified and improved to highlight the perspectives necessary for the FinTech adoption process.

In today's increasingly digital world, the risk of cyberattacks is growing, and financial organisations must take adequate measures to protect against these threats (Carlson, 2015; Davis, 2017). Cybersecurity is especially crucial in the FinTech sector to maintain a competitive edge and prevent disruption of business models. As institutions adopt the FinTech paradigm, cybersecurity becomes essential to their strategy, design, and operations in today's fast-paced environment. Cyber-attacks on FinTech services can have severe consequences, causing economic, social, and organisational damage and eroding customers' trust (Kranz et al., 2013; Möller et al., 2012). The use of mobile technology has grown significantly since 2013, leading to the convergence of mobile devices, the internet, and integration. The Data Breach Investigations Report 2021 (Bassett et al., 2021) highlights the state of data breaches in Europe, the Middle East, and Africa (EMEA), emphasising the importance of strong cybersecurity measures.

There are few systematic literature reviews on FinTech and its relationship to cybersecurity. A study conducted by Zavolokina et al. (2016) suggests that FinTech involves more than just IT in finance and can be classified into various categories such as start-up, service, technology, enterprise, digitalisation, industry, new generations, opportunity, product, and risk. Additionally, Stewart & Jürjens (2018) found that insufficient cybersecurity measures can impact individual confidence in adopting FinTech due to data security and trust concerns. Meanwhile, Mehrban et al. (2020) thoroughly analyse FinTech's privacy and security issues, including current security concerns, detection mechanisms, and proposed security solutions.

The FinTech industry faces various cybersecurity threats that can result in financial losses, damage to reputation, and legal issues for companies (Najaf et al., 2020; Barbu et al., 2021; Kaur et al., 2021). Researchers have suggested different cybersecurity measures that FinTech companies can adopt to safeguard themselves and their customers from cyberattacks (Najaf et al., 2020; Kaur et al., 2021). Additionally, Taylor et al. (2020) have discussed the future of blockchain and cybersecurity research, education, and practices in this field. Vučinić et al. (2022) have introduced a FinTech SWOT analysis matrix to evaluate strengths, weaknesses, opportunities, and threats. They have also recommended

using "risk-based thinking" as a management strategy to tackle the challenges and opportunities in FinTech. Finally, Vučinić et al. (2022) have examined cyber risk as the latest and most significant issue in the FinTech sector during these uncertain times.

While much literature is available on FinTech innovation, some studies have identified areas for further research. For instance, certain studies have focused exclusively on specific cybersecurity threats or countermeasures, while others have only considered the perspective of FinTech organisations, neglecting the viewpoints of consumers and regulators. Additionally, some studies have analysed the legal frameworks governing cybersecurity for FinTech organisations. However, these frameworks may not be comprehensive enough to address all the FinTech industry's cybersecurity concerns (Najaf, 2020). Such research is crucial in enhancing the understanding of academics, industry players, and regulators on safeguarding digital products and services against cybersecurity threats.

The research paper 1 in this thesis surveyed 308 FinTech users and innovators on their attitudes towards FinTech adoption. The results showed that the perception of the risks and benefits of FinTech influences the willingness to adopt FinTech. The study also found that the number of mobile phone users is increasing rapidly, but the adoption of FinTech is slow. Interestingly, only 10 % of the respondents knew FinTech, although 99 % own mobile devices. Furthermore, less than 1 % of the participants embrace FinTechs, which is worrying. The empirical results confirm that data security, customer trust and the user design interface affect the adoption of FinTech. The TAM was used to test all hypotheses in this paper. More information on the TAM can be found in section 2.6.

In the next section, this study delves into cloud computing, which serves as the primary means of data storage and processing in the FinTech industry and explores the various challenges cyber threats pose.

2.3. Cloud computing

According to the U.S. National Institute of Standards and Technology (NIST) definition as provided by Mell and Grance (2011), cloud computing refers to delivering on-demand computing services over the Internet to provide rapid innovation, agile resources, and economies of scale (Mell & Grance, 2011, p. 2). This model has three service and four deployment models - public, private, hybrid, and community. These models are associated with three integration models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) (Modi, 2013; Stewart, 2021). Each delivery and model present its challenges in terms of risk exposure.

A specific cloud user operates a private cloud, while a public cloud is run by the cloud provider and leased to cloud users. A community cloud is used by organisations collaborating and sharing the same goals, and a hybrid cloud is a combination of private and public clouds that provide a higher level of adaptability, availability, security, and privacy. An example of hybrid cloud deployment models are companies with strict security requirements, such as financial institutions or healthcare. Here, sensitive data is stored and processed in an internally managed private cloud, while less sensitive data or applications such as customer relationship management (CRM) are stored in a public cloud for scalability and cost efficiency (Mell & Grance, 2011; Yang & Tate, 2012). The three most common cloud infrastructure models are IaaS, PaaS, and SaaS. In the IaaS model, a cloud user exploits the computing, storage, or network infrastructure. In PaaS, a cloud user uses the sources the cloud provider provides to run various applications. In SaaS, a cloud user uses software applications that run on the cloud provider's infrastructure.

Cloud computing has a clear advantage over traditional in-house computing resources because it can be scaled according to demand. This is made possible by dynamic, usage-based pricing models agreed upon by providers and users in subscription contracts. In essence, cloud computing can be seen as IT outsourcing that offers greater efficiency, lower costs, and higher flexibility (Leimeister et al., 2010, p.7). Companies can effectively serve customers with readily available and scalable computing resources while reducing fixed IT costs. Furthermore, this can lead to the development of innovative services and new business models that have the potential to be ground-breaking for customers. The use of sophisticated tools can also ensure that customer expectations are met and exceeded without significant upfront investment (Müller et al., 2015).

According to a literature review by Müller and colleagues (2015) based on Pearlson & Saunders' 2007 work, cloud computing benefits can be utilised at various levels of business IT maturity. The first level involves reducing costs and improving business process efficiency to increase efficiency. The second level focuses on improving business effectiveness by enhancing collaboration within the organisation, integrating business and IT infrastructure, and emphasising core competencies. The third level highlights how cloud computing can promote innovation and business transformation by facilitating growth through innovative services and products, agile capabilities, and increased collaboration with business partners. Additionally, cloud computing promotes more information sharing and knowledge networks across the value chain by connecting stakeholders through shared systems and more accessible data.

Apart from the benefits, cloud computing also carries potential risks and costs that can outweigh those benefits. In research paper 2 of this thesis, 208 IT executives from regional and large commercial banks were asked about their views on adopting Infrastructure as a Service (IaaS). The survey found that the perceived risks and benefits of IaaS can impact IT managers' intentions to increase their current level of IaaS adoption. The research modelled the internal and external components that influence the adoption of IaaS by determining the internal-external factor (IEF). The primary technical acceptance model (TAM) constructs, perceived usefulness (PU or U) and perceived ease-of-use (PEOU or E), represent the internal elements determining IEF. According to TAM, PU is the individual's belief that he or she can adapt to a new technology more efficiently (Davis, 1989; Venkatesh et al., 2003), while PEOU is the belief that a new technology is easy to use. In this respect, the financial sector will choose IaaS if it is valuable and effortless. Therefore, the research characterised IEF as an arbitrary extension in terms of U and the ability to use IaaS with less effort (PEOU). In this way, the IEF captured the TAM variables PU and PEOU as antecedents of the intention to use IaaS. This is similar to theory of reasoned action (TRA) because of the aggregation of effort and usability but differs from TAM (Fishbein & Ajzen, 1975), where the two constructs are treated differently (Pikkarainen et al., 2004). The external determinants of IEF were determined by the efficiency of assured connectivity and coverage, which provided banks in this research with easy and consistent access when moving to the cloud (Venkatesh et al., 2003). In this work, several hypotheses were put together for testing. The survey model assessed the impact of various beliefs related to performance, economic, strategic and management risks, and beliefs related to opportunities such as cost benefits, strategic flexibility, focus on core competencies, access to specialised resources and quality improvements. The results showed that managers were significantly affected by economic, performance and strategic risks, while management risks did not significantly impact them. In addition, security risks such as data loss, theft or corruption were cited as the most essential factors for adopting Infrastructure as a Service (IaaS).

Even though both cloud and on-premises infrastructures are exposed to the same threats, the data stored by cloud providers has become an attractive target for attackers as the number of cloud users has grown. The field of cloud computing security is vast and covers a multitude of concerns. These include safeguarding hardware and platform technologies and securing access to cloud data and resources through various end-user devices. Furthermore, its security and privacy issues have always been a significant concern for many cloud customers (Kaufman, 2009). These concerns have hindered businesses and organisations' widespread adoption of cloud computing. The need for increased protection and security of data is not only critical for cloud computing deployments but also for

businesses and individuals who rely on computing resources. The number of data breaches and associated losses has increased, which further highlights the need for security. Although cloud computing enables DT, information security and privacy also play a more diverse and sometimes equivocal role - as obstacle, barrier, target, or pillar - which is explored in the section 2.4.

2.4. Information Security Management

US NIST defines information security as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction to ensure confidentiality, integrity, and availability (Paulsen & Byers, 2019). ISO/IEC 27000 defines information security as maintaining the confidentiality, integrity, and availability of information, but may also include other attributes such as authenticity, accountability, non-repudiation, and reliability (ISO, 2018, p. 4). The CIA triad, which stands for confidentiality, integrity, and availability, is a common acronym for explaining the three information security principles. Confidentiality ensures that information is not disclosed to unauthorised persons or processes, integrity protects against improper modification or destruction of information, and availability guarantees timely and reliable access to and use of information (Paulsen & Byers, 2019; Winniford, 2009; Barlette & Fomin, 2008).

Information security is essential to IS researchers and practitioners, particularly when discussing significant security or privacy issues within an organisation (Winniford, 2009; Barlette & Fomin, 2008; Lowry et al., 2017). Researchers in the field of Information Systems contend that security and privacy are more crucial than ever and have garnered attention from managers due to recent advancements such as the Internet of Things (IoT), the growing use of artificial intelligence (AI), and the overall reliance on information systems and networks (e.g., Chen et al., 2011; Lowry et al., 2017). The sophistication of threats and their associated scale, severity of impact and cost are constantly increasing due to the growing importance of information and information systems to individuals and organisations, providing an ever-larger attack surface (e.g., Barrett, 2019; Salge et al., 2015). As a result, information security managers have made information security and risk management a top priority in their organisations (Guo et al., 2012; Harrington, 1996 & Straub et al., 1990). This can be seen in the development of standards and codes of practice, such as ISO/IEC 27001 (2022) and various research papers, such as those by Straub & Welke (1998) and Solms et al. (1994).

Therefore, managing information security is an essential part of managing organisational risks. It ensures that business operations continue without interruption and protects the privacy of both employees and customers. Security measures are implemented to preserve information and data

confidentiality, integrity, and availability. Privacy is considered a fundamental right that involves handling personal data lawfully and responsibly, following policies, public sentiment, and legal guidelines.

Previous studies on the deployment of information security measures have indicated that their successful implementation depends on various factors such as technological, organisational, environmental, and individual factors. For instance, at the environmental level, security breaches and the announcement of IT security investments may either result in the absorption of market share and power by unaffected competing organisations or trigger IT security investments among competitors in a contagion effect (Jeong et al., 2019). Herath and Rao (2009) suggest that organisations use various methods to improve data security. Ifinedo (2012) points out that many companies focus exclusively on technology-based measures, which are only effective if employee behaviour is considered. Crossler et al. (2013) recommend a strategic approach that combines technological, human, cultural and organisational factors for information security management. This approach emphasises the importance of both technology and employee behaviour in creating a secure environment. Research has found that the successful implementation of information security measures is driven by various factors, including technological, environmental, organisational, and individual factors. Environmental factors, such as security breaches or IT security investments, can affect market share and spur investment among competitors. It is important to consider the role of individuals in information security, as employees lacking risk identification skills can put organisations and their data at risk (e.g., Willison & Warkentin, 2013; Crossler et al., 2013). However, individuals within organisations also make decisions about security measures and technology adoption, which can carry inherent security and privacy risks (e.g., Angst et al., 2017; Lowry et al., 2017). Business goals are intertwined with information systems, so every IT investment or outsourcing decision must consider security and privacy concerns (Milovich, 2019). Da Veiga and Martins (2015) conducted a questionnaire to explore how human, technological, and strategic controls are interlinked. To collect data, they used an information security culture assessment (ISCA) based on a case study of an international financial institution. The study was conducted over eight years and covered twelve countries, with data collected at four intervals. The focus of the study was on the impact of security awareness training. The researchers recommended additional research on employees who adhere to information security policies and those who do not. Additionally, they recommended expanding the study to include national and cultural differences.

Numerous studies have revealed that many organisations overlook the importance of human behaviour in managing information security, leading to security breaches. Webb et al. (2014) proposed a model called situation-aware ISRM (SA-ISRM) to supplement the information security risk management (ISRM) process. However, their model only focused on ISRM deficiencies and failed to consider security policy compliance based on individual employees. Similarly, Li et al. (2010) argued that recent studies on information security management neglect the perceived benefits of degenerate behaviour, individual norms, and organisational settings. Their research model utilised an online survey sent to organisational employees, focusing only on compliance with the internet use policy (IUP). Their work highlighted the risks posed by non-compliant employees in an organisation's security management context. They also recommended considering compliance decisions based on cost-benefit analysis limited by individual standards and organisational setting factors. However, neither Li et al. (2010) nor Webb et al. (2014) fully encompassed all the elements of human behaviour and social structure in an organisation, such as human ability, culture, IS management, top personnel, and technology, and how all these factors interrelate and work together. Consequently, their studies indicate the limitations of theory-based empirical studies on employee security policy compliance, which is addressed in the next section.

2.5. Information Security Policy

An information security policy (ISP) is a set of guidelines and procedures that regulate employee behaviour. It establishes a standard for the appropriate use of the organisation's information technology, such as networks and applications, to ensure data confidentiality, integrity, and availability (Doherty & Fulford, 2006). Due to the increasing security threats organisations face worldwide, reliable information system operation is more crucial than ever. To safeguard their valuable information, organisations require security controls. According to Hone and Eloff (2002, p. 402), an ISP is the most critical security control, and according to Whitman et al. (2001), developing an information security policy is the first step in preparing an organisation for internal and external attacks. Some believe management security policies are more effective in reducing computer security incidents than many electronic devices (Buss & Salerno, 1984). The ISP is a governing document that defines an organisation's overall boundaries of information security (Sohrabi et al., 2016; Lucila, 2016). It also demonstrates management's commitment to and support for information security in an organisation and the role it plays in achieving and supporting the organisation's vision and purpose (Sohrabi et al., 2016; Knapp et al., 2009; Kadam, 2007; Lucila, 2016). Management endorsement, relevance to the

organisation in question, practicality, achievability, flexibility and enforcement, and the fact that the policy includes all relevant parties are all aspects that contribute to a successful ISP.

The importance of policy documents has been extensively discussed in the literature, but there remains a debate on their structure and key elements. Previous studies have explored policy structure from conceptual perspectives, with some scholars proposing single policies while others suggest dividing them into subdocuments. Additionally, there is a focus on the difference between high and low levels of policy practices, though guidelines should address both means and ends (Baskerville & Siponen, 2002). More studies have been conducted on effective configuration for information security documentation, but the issue has become more complex with the introduction of new forms of security documents. This calls for a focused, empirical study to examine the structural arrangements of information security policies currently being adapted and practised by organisations.

While the structure of information security policy has been discussed in the literature, there has been limited academic discussion about issues that need to be addressed. The international standard 17799 ISO:2005 indicates the types of issues that can be addressed, but there is still a lack of empirical contributions and consensus on academic security. In addition to concerns regarding structure and content, there are also concerns about policy effectiveness. Many organisations claim to have developed and implemented information security policies, but high degrees of information security incidents and breaches suggest a lack of policy effectiveness and/or communication. One possible reason is that organisations follow narrow policies focusing on confidentiality, integrity, and availability, ignoring important human and organisational aspects. Overall, there is a need for a more comprehensive and consistent approach to information security policy that addresses both technical and human factors.

Organisations heavily rely on information technology (IT) to carry out daily tasks and critical operations, making it essential to have an ISP for business continuity. A robust security framework is necessary to achieve ISP goals, ensuring that critical information assets are kept confidential, integral, available, authentic, authoritative, verifiable, and non-repudiated (Alhanahnah et al., 2016). The ISP establishes an organisation's approach to securing information assets from unauthorised access, exposure, corruption, and alteration (Mauritian, 2011). Policies are typically implemented to monitor the exposure and misuse of information, and international security policy templates are available to serve as preparatory tools for policy development (Goel & Chengalur, 2010; Baskerville & Siponen, 2002).

Developing a security strategy is often time-consuming, challenging, and costly (Waddell, 2013; Goel & Chengalur, 2010). Replicating an ISP from another entity may not be sufficient to address specific concerns, and even a well-replicated policy may fall short under certain circumstances (Bjorck, 2004; Kusserow, 2014). Therefore, ISP strategies must be customised based on the organisation's culture, beliefs, operations, environment, and policy requirements (Siponen & Willison, 2009; D'Arcy et al., 2009). It is vital to consider various factors when formulating and developing ISPs, such as different types of facilities, users, management support, technological changes, social concerns, cultures, and economic, legal, and political aspects (Goel & Chengalur, 2010).

Although technology has significantly advanced in ensuring information security, human error remains a weak point in the security chain (Stewart, 2020). Research has shown that employee threats pose one of the most significant risks to information security in recent years (Mattord et al., 2014). Studies have found that insiders are responsible for 40% of all data breaches worldwide, causing more harm than outsider attacks (Singh et al., 2016; Gelles, 2016). Most insider threats arise from poorly defined or absent ISPs. Eloff & Eloff (2005) suggest that a holistic approach to information security is necessary to prevent security breaches. Experts recommend two vital elements in developing a well-defined ISP: the development process (Tuyikeze & Flowerday, 2014; Flowerday & Tuyikeze, 2016; Lucila, 2016) and the content of the ISP (Doherty et al., 2011; Maynard & Ruighaver, 2006). An effective ISP should convert management expectations into measurable and distinct objectives and demonstrate their validity, legibility, and sustainability (Goel & Chengalur, 2010).

While many academic papers have discussed the structure and content of an ISP (Tuyikeze & Flowerday, 2016; Lucila, 2016), few have explored the step-by-step process of developing a strategic ISP for a multinational company, which is the focus of this paper. Establishing an effective ISP requires consideration of factors such as the needs of the business and relevant laws and regulations (Wiander, 2009). Security experts agree that implementing and enforcing security policies is critical to maintaining and protecting information systems. Two elements that impact the effectiveness of an ISP are its development process and content. Therefore, improving existing practices is critical to improving the overall quality of strategic security policies. The attitudes and behaviours of those involved in the development process also play a role. It is important to recognise that different stakeholders may have different perceptions of quality, and addressing these perceptions is essential for improving ISP development (Knapp et al., 2009; Sohrabi et al., 2016).

To develop an effective ISP, two elements of ISPs that affect their effectiveness are the development process and the content (Flowerday & Tuyikeze, 2016; Tuyikeze & Flowerday, 2014; Lucila, 2016; Stewart, 2020). Improving existing practices is important for the quality of strategic ISPs. In other words, it examines how organisations create, implement, use and sustain strategic security policies and seeks to change organisational practices to improve the overall quality of emerging policies. As with many organisational efforts, the behaviour and attitudes of the individuals involved have an influence. In addition, recognising that different stakeholders have different perceptions of quality and enabling the correction of these perceptions is critical to improving ISP development. This study focuses on ISP development in an organisation. Companies need to implement security programmes to protect their information systems in response to the growing number of cyber threats. It is, therefore, crucial that they have well-developed information security strategies. There is, therefore, a need for scientific research in this critical area. Using a qualitative approach, Paper 6 of this thesis proposed a research model that holistically combines six constructs, latent variables, and factors from previous research models to improve ISP development and compliance in multinational organisations. This research paper (Paper 6) is dedicated to the study of ISP development in an organisation.

2.6. Technical Acceptance Model

The TAM is a widely recognized framework for evaluating technology adoption plans. The goal of the model is to identify the factors that drive computer usage (Davis, 1989; Yang, 2005). Davis et al. (1989) used the TAM to model the relationship between these factors and formulate hypotheses. They found that perceived usefulness and perceived ease of use are the main determinants of an individual's expectation to use new technology. Perceived usefulness is the extent to which individuals believe that using a particular technology would improve their work performance, while perceived ease of use refers to the convenience of using the technology (Davis, 1989). In short, an individual's intention to use a new technology is influenced by how useful and easy it is perceived to be. Davis' research showed that the relationship between usage and usefulness is stronger than the relationship between use and frequency of use. Although TAM is considered a robust model, several researchers have analysed its validity and shortcomings, including TRA and TPB (Ives & Olson, 1984; Venkatesh & Davis, 2000). The TRA was developed by Ajzen and Fishbein (1980) to explore the factors that influence an individual's behaviour when using certain technologies. TRA acknowledges behaviour and subjective norms as essential indicators of a person's intention to use a particular technology. According to TRA, an individual's behavioural intention is a combination of their attitude towards the behaviour and

perceived normative factors. This model refers to an individual's performance on the behaviour as an attitude, rather than their overall performance (Fishbein & Ajzen, 1975). The subjective criterion is the person's belief that a person important to him or her believes that they can carry out the implicit behaviour. However, TRA alone is not suitable for this research because it assumes behaviour when the individual's conscious control is compromised (Ajzen, 1991). Furthermore, it is not capable of identifying relevant beliefs for a specific behaviour. According to Straub et al. (1997) and McCoy et al. (2007), TAM may not be universally applicable, as it was mainly developed in the United States and may not accurately predict technology adoption in different cultures. Venkatesh and Davis (2000) developed TAM2 to overcome these limitations, which integrates social impact and cognitive tool-based techniques as fundamental components of adopting information systems. However, TAM's U and E components have been criticised for ignoring the main factor hindering information system adoption (Luarn & Lin, 2005). To address this issue, Luarn & Lin (2005) proposed integrating elements of consumer trust (perceived credibility) and two wealth elements (perceived self-efficacy and perceived financial cost) into TAM, as consumer trust indirectly influences customer intention to adopt new technology based on E.

Papers 1 and 2 of this study integrated data security into the TAM, as data security is the most important determinant of consumer trust in IS. It is clear here that a need for more information security awareness is a barrier to adopting FinTech and IaaS. Tang et al. (2004) and Wang et al. (2003) explored the impact of data security and privacy concerns on mobile banking adoption using the TAM as a blueprint. Stewart & Jürjens (2018) highlighted data security and consumer trust as essential determinants of technology adoption. As mentioned above, the two different TAM constructs were merged with the TRA model to form the internal-external element (value creation) construct in this study. Therefore, in this study, the elements that affect IaaS and FinTech are explored by extending the TAM to include the elements of the proposed Nine Five Circle (NFC) factor (data security and consumer trust); both Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al., 2003) are excluded due to its complexity (Venkatesh et al., 2003). In addition, UTAUT examines the construct of social impact, which is not needed in the current work.

2.7. Cybersecurity as social problem

Attacks on information security using social engineering and other tactics targeting human weaknesses in the security chain are becoming more common, reflecting this. Technical solutions alone are not sufficient to ensure information security in the DT. Therefore, it is necessary to assess the human component of security. It has been shown in various studies that more than a human-centred approach to cyber security is needed (Stewart, 2022; Holgate et al., 2015; Mujinga et al., 2012; Paja et al., 2017).

The complexity of the pervasive online behaviour of individuals and organisations presents numerous information security risks (Davis et al., 2014). Individuals and organisations increasingly store and transmit sensitive and confidential information on various networked devices. This information is transmitted over the internet, a public, open and global network. However, technical solutions to protect critical information assets - including devices, transmission media and data - are insufficient if other factors, such as the human factor, are not considered. Therefore, information security is now considered holistically to include technological and social aspects. This argument focuses on the unpredictable nature of human behaviour, which cannot be adequately formulated due to various factors, including computer knowledge and mental information security models (Yee, 2004). This has led to information security being treated as a cross-disciplinary field (Sveen et al., 2009), combining expertise from computer science, engineering, social sciences, and many other fields.

2.7.1. Humans as 'Weakest Link'

Human behaviour is still considered the weakest link in the cyber security chain and has become the main target of many cyberattacks (e.g., D'Arcy et al., 2009; Schneier, 2011; Crossler et al., 2013). The interaction between humans and IS represents a significant security risk (Elhai et al., 2017).

Understanding user behaviour should help design and develop an information system to accommodate human behaviour. Understanding the role of humans is crucial for information security systems, as they usually rely on user interaction to create a secure environment and protect information assets from attackers. Thus, relying on technical solutions without considering human factors creates a gap in the relationship between humans and technology, which also impacts the security of IS. According to Furnell (2005), users find it challenging to adhere to security policies due to the system architecture and the nature of the security tasks. It should be noted that gender (e.g. Anwar et al., 2017), motivation (Guo et al., 2011), attitude (Bulgurcu et al., 2010), professional and technical skills (Carlton, 2016), organisational culture (Hu et al., 2012), perceived gravity and control beliefs (Workman et al., 2008),

peer pressure (Dang-Pham et al., 2017), individual accountability, strategy of intervention and pre-knowledge (Shillair et al., 2015), and perception of personality (Shropshire et al., 2015). According to Tarazan & Bostan (2016) age and demographics may indicate how well they comprehend security warnings and the proper course of action. Security can be intricate and challenging to comprehend, but it is also simple to abuse (Sasse et al., 2001).

In addition to end-user perceptions of vulnerabilities (e.g., Furnell, 2005; Tarazan & Bostan, 2016), security flaws in app design and development can also be found on highly secure websites that developers ignore (Newhouse et al., 2016; Stewart, 2022), such as requesting login options on insecure websites, storing data unencrypted, and sending sensitive information in plain text via email or an unencrypted protocol (D'Arcy & Devaraj, 2012; D'Arcy et al., 2014; Luo et al., 2011).

Hence, information security must incorporate human factors to achieve the desired goals. The success or failure of information security thus depends on how humans use information security processes (Crossler et al., 2013). Human engagement underlines the need to consider the social dimensions of information security, as more than technical solutions are needed. For these reasons, an IS that addresses information security and trust, and usability is essentially a socio-technical system that needs to consider the social behaviour of users in addition to the technical functions of the system (Holgate et al., 2012; Mujinga et al., 2017). In general, users of computers and digital products want their system to protect their data without their intervention. Therefore, security, trust, and usability must coexist and complement each other rather than contradict each other in protecting IS (Stewart & Jürjens, 2018; Stewart, 2022).

2.7.2. Socio-Technical System Theory Approach to Information Security (STS)

The need to consider socio-technical aspects is even more important in information security systems, as the end-user of all IS plays an essential role in the security chain, regardless of which advanced security model is chosen. For example, advanced encryption techniques critical to data security can make IS technically secure. However, these techniques can fail if abused or circumvented by users. Thus, technical defences are inadequate against social attacks such as social engineering. Hence, the need for a socio-technical strategy that relies heavily on human elements is highlighted by the complexity and difficulty of providing adequate security in the face of these various components. This socio-technical definition describes information security systems for web applications and mobile apps very precisely so that their design can be improved by applying this method. This forces developers to balance

usability and information security goals so that end users can use IS successfully and efficiently, especially information security systems (Holgate et al., 2012; Mujinga et al., 2017; Paja et al., 2015).

A more complex system emerges when humans and technology work together (Davis et al., 2014). Unlike traditional models and methods, STS theory strives to address some of the key challenges raised by traditional and technical models. Modern business environments have increased complexity in many organisations, affecting their productivity and effectiveness in identifying associated security risks. The STS approach aims to allow organisations to carry out joint optimisation, giving equal weight to technical and human security factors (Chen & Redar, 2014). This entails examining the organisation's current information and cyber security practices and classifying each output control as social, technical, human, or environmental. When a security solution is discovered with an excessive focus on the social or the technical, an STS gap exists. The model aimed to detect and close STS gaps, allowing organisations to achieve collaborative optimisation. These kinds of STS gaps are tantamount to system vulnerabilities that cyber-attackers can exploit. STS theory is based on perceiving both "socio" and "technical" components as companion pieces of a complex system. An organisation concentrating on a single part of the system needs to analyse and comprehend the system interconnections. This theory considers the function of human factors in IS security as a key factor in detecting and preventing data breaches (Emery, 1982; Mumford, 2006). Accordingly, humans are the weakest link in the security chain and are critical to cyber security. Although many humans view technology as a factor in cyber security, STS theory effectively designs a system's environment and security by examining goals, culture, technology, humans, infrastructure, processes, procedures, usability issues and internal security governance. As a result, STS theory can be used to investigate how individuals contribute to an organisation's security depending on how they view and handle information system security. STS systems emphasise adaptability, aiming to change individuals' behaviour and how they deal with uncertainty (e.g., phishing emails). The STS theory emphasises the responsibility of the individual and the group or team that shares responsibility and can work together, resulting in fewer silos and often more effective communication. According to STS theory, individuals strive to take responsibility for their actions, for example, by not clicking on phishing emails or sharing sensitive information with humans who are not authorised to receive it. In this way, the individual is empowered to make choices. STS consist of distinct levels: Organisation, Society, Business Processes, Equipment, Operating System, Data Management, Communication and Application, but all these levels function as part of the overall STS and influence and impact other levels and systems outside the STS.

So far, attention has been focused on the separate components of the socio-technical system (structures, humans, technology, and tasks). However, this study contends that most attacks on information system security occur because of subsystem interaction. The assault landscape is set up so that a perpetrator can use the weakest link in the chain, generally humans, to circumvent existing laws and avoid all available threat detection systems. The rapid development of technology has changed humans's activities, laws, and opportunities. At the intersections of subsystems, there is potential for attacks on the security of information systems. In addition, an insufficient understanding of how the different levels interact can increase the organisation's risk of disasters, leading to a less effective response to environmental changes or other challenges. The effectiveness of STS depends on an organisation's ability to comprehend how the different levels affect each other and to prevent the emergence of silos that could separate the systems and reduce their effectiveness. Another negative factor is the need for more management control of the STS and the inaccuracy of information that could affect decisions on security measures. Nonetheless, STS neglects certain coding practices and application security in general, all of which play a more significant role in DT security, as well as the usefulness, authenticity and validity of the information contained in the processes (Stewart, 2022; Holgate et al., 2012; Mujinga et al., 2017; Paja et al., 2015).

According to Ferreira et al. (2014), an effective security system is secure even when used by individuals. The literature claims that creating such systems is becoming increasingly complex, especially given the diversity of user groups and the increasing reliance of cyber criminals on social attacks. Even the most sophisticated technical security measures are rendered useless by the human element, mainly because system users need to prioritise information security. This paper argues that we can resolve the conflicting issues between information security and usability by implementing an STS strategy along with ISO27001 standards and NIST. It is widely recognised that technological solutions to information security and cyber security issues, while important, are not sufficient to solve both problems in complex socio-technical systems (Stewart, 2022; Holgate et al., 2012; Mujinga et al., 2017; Paja et al., 2015).

2.8. NFC Model

Despite the significance of IS security research and practice, current approaches have focused on isolated aspects rather than a holistic approach. As Stewart (2022) pointed out, this approach has resulted in demands for a holistic approach that integrates technology, humans, and processes to

protect organisations from cyber threats. In today's digital age, all organisations are required to have a comprehensive cybersecurity strategy (Bakar et al., 2021; García-García et al., 2021; Khan et al., 2022; M'baya et al., 2017; Tervoort et al., 2020). While technology tools are useful, incorporating corporate culture and human factors into the security perimeter is equally important to combat the increasing data breaches and related costs. For this reason, the NFC holistic model was developed, combining all aspects of strategy, constructs and success factors discussed in the six papers. Each of the six papers provide a description of how the model was utilised within its content.

The holistic NFC cybersecurity model aims to improve an organisation's security performance and outsourcing by focusing on operational, information, and cyber security. It highlights the importance of analysing the relationship between technology and human factors through risk analysis. Additionally, it enables the measurement of information technology security and the evaluation of an organisation's digital strategy's security performance. Ultimately, the model aims to enhance information security in human-technology interaction. Stewart & Jürjens (2017) have utilised it to represent an organisation's ISMS. Additionally, it has helped identify obstacles in financial technology and suggest practical solutions (Stewart, 2018). Stewart (2021) has employed it to evaluate technology transfer in the context of cloud innovation while proposing a systematic methodology for developing and sustaining ISPs (Stewart, 2022). NFC has also helped enhance software testing, verification, and reliability (Stewart, 2022) and develop a security strategy for DT (Stewart, 2022). As shown in Table 1 and Figure 3, the model comprises three phases (stages), namely: (i) situational awareness, (ii) integration control and (iii) gap closure. These stages are called defence-in-depth, also called layered or NFC defence. Situational awareness defines the security challenge and its underlying variables, as shown in Table 1.

Table.1 NFC Lifecycle

	Phase	Subjects
Phase 1	Situational Awareness	<ul style="list-style-type: none"> ● Know what it should be. ● Track what it is. ● Infer when <i>it should be</i> and <i>does</i> not match. ● Do something about the differences
Phase 2	Integration Control	<ul style="list-style-type: none"> ● Cybersecurity programme establishment, ● Risk assessment ● Risk treatment, ● Cybersecurity assessment

		<ul style="list-style-type: none"> ● Controls
Phase 3	Gap Closure	<ul style="list-style-type: none"> ● Monitoring ● Improvement

The integration control phase includes cybersecurity programme development, risk assessment, and control measures. The gap closure phase involves implementing and monitoring to ensure the process is completed effectively and aligns with the organisation's security strategy. The security challenge and its underlying variables (see Table 2 in section 2.10) are defined by situational awareness. The phases of cybersecurity programme development, risk assessment and control measures comprise the integration control phase. In contrast, the gap closure phase includes the implementation and monitoring required to ensure that the overall process is completed effectively and is consistent with the organisation's security strategy.

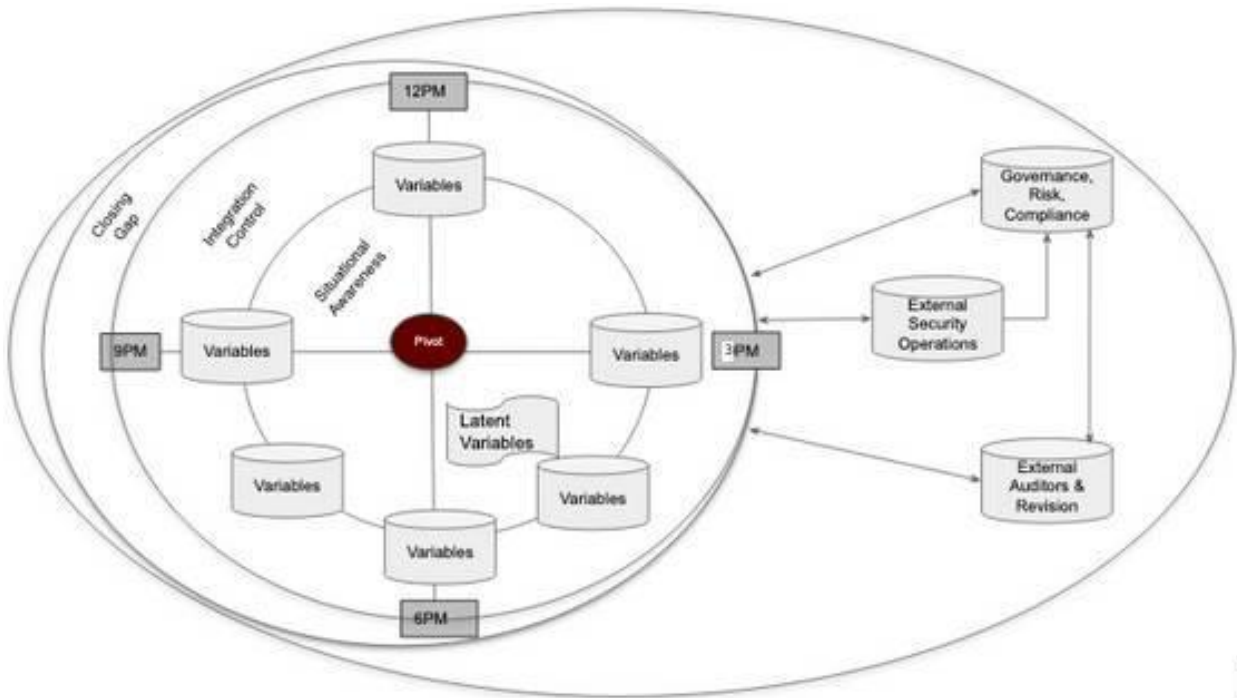


Fig. 3. NFC Information and Cyber Security Management System Model (ref., Stewart, 2017)

Other external variables shown in Figure 3 include (i) the established policies that affect the rules and regulations within the organisation; (ii) the external audit of compliance that affects the field of knowledge, the type of practices that affect cybersecurity and the knowledge management processes

in place; this includes benefits, costs, and relevant services; and the technological aspect that relates to the role of enabling technologies.

The NFC model bridges the theoretical gap between DT cybersecurity (Angelini et al., 2015; Gomber et al., 2018). By combining DT strategy theories with cybersecurity best practices (Schneier, 2015), this research ensures that DT initiatives are designed to be secure from the start (Stewart, 2022). The NFC model is based on advanced cybersecurity theories and leverages emerging technologies to improve organisational security in the digital age (Dhillon & Backhouse, 2000). The model incorporates various security measures and protocols to improve the security posture of organisations amid DT. These theoretical foundations show how the model uses cutting-edge technologies to improve organisational security (Arbanas et al., 2019; Angelini et al., 2015).

The NFC model is based on established cybersecurity theories, including the CIA triad (Arbanas et al., 2019). By grounding the NFC model in these foundational theories, the model advances the field's ability to apply these principles in the context of DT (Schneier, 2015). These theoretical foundations underpin the scalability and applicability of the NFC model in various organisational settings (Ande et al., 2020). The theoretical concept of adaptability and usability underpins the modular nature of the NFC design and ensures that it can be adapted to the unique needs of different sectors and organisational sizes (Andriotis et al., 2015; Wang et al., 2008; Muehe & Drechsler, 2017). The research synthesises cross-disciplinary knowledge from risk management, organisational theory and computer science. The NFC model draws on theories from these different fields and provides a holistic view of cybersecurity in DT, emphasising the importance of technological and organisational aspects (Andriotis et al., 2015; Wang et al., 2008; Mühe & Drechsler, 2017).

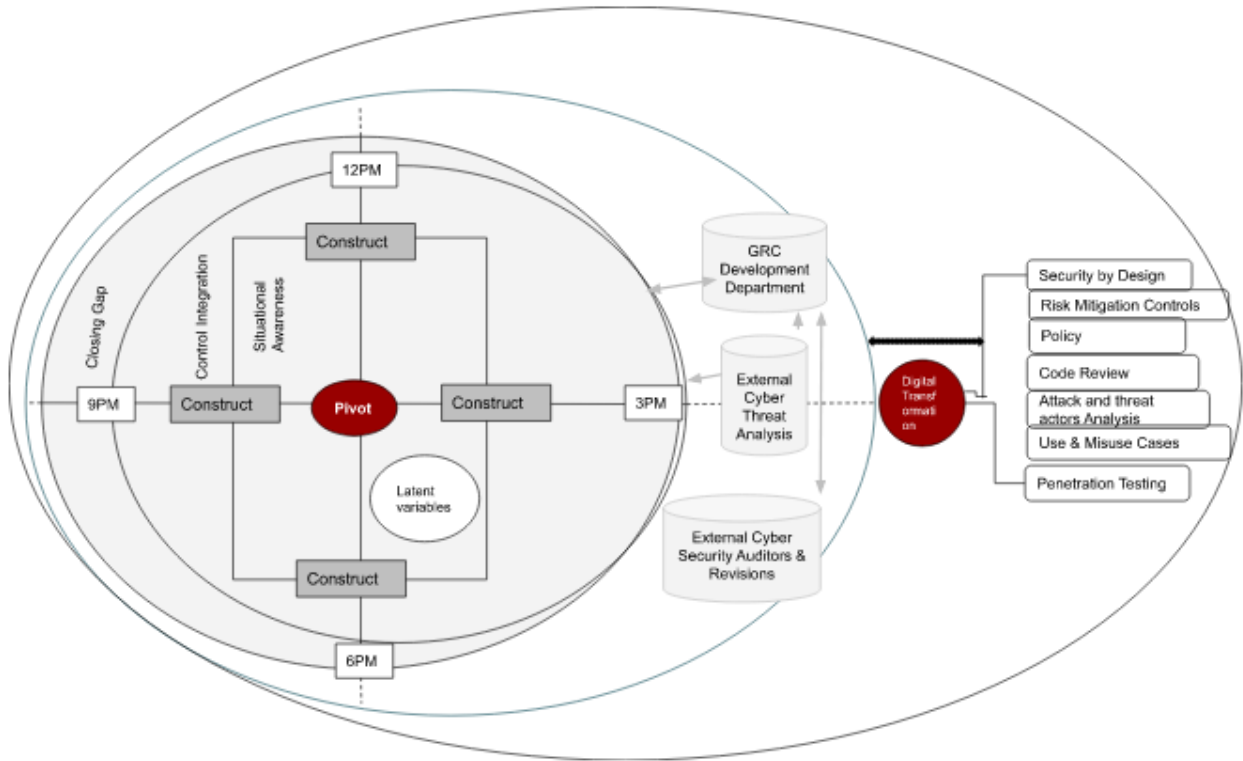


Fig. 4. NFC Information and Cyber Security Management System Model for software security (ref., Stewart, 2017)

Figure 4 below is an expanded version that includes the security components for the software used and the software development process. As shown in Figure 4, the model is examined through Security by Design, with code review and penetration testing of great importance. This has already been presented in papers 3 (Chapter 6) and 4 (Paper 7). The white/black box testing, and external audits ensure that the implemented security strategy improves the knowledge domain, the engineering-oriented procedures, and the existing knowledge management processes, including benefits, costs, and relevant services, as well as the technological aspect concerning the role of enabling technologies. The audit is conducted at regular intervals to determine the project's maturity. According to Ishikawa (1985), "failure to revise standards and regulations is evidence that no one is applying them seriously". Each construct of the work is analysed and prioritised by comparing impact with probability during each life cycle.

In addition, there is a horizontal activity, also called latent variables, directly linked to all three phases: communication, culture, trust, privacy, and consultation activities. These latent variables are options that the organisation can substitute depending on its current gaps and needs. The variables and latent

variables are determined based on the data collection. Section 2.10 explains the life cycle and development process of NFC.

2.9. Literature Summary

Organisations across industries have made digital transformation a strategic imperative in recent years. However, they encounter various cybersecurity challenges as they adopt technology to improve their operations, products, and services (Crossler et al., 2013). This literature review highlights the crucial findings and themes in cybersecurity ((Bongiovanni, 2019) and DT (Hess et al., 2016).

DT is a fundamental shift in companies' business, using cutting-edge technologies such as cloud computing, IoT, AI and data analytics (Barringer & Harrison, 2000; Wilkinson et al., 2004). It is driven by the need to remain competitive and agile in a digitalised world. However, integrating digital technologies into core business processes and increasing connectivity creates new vulnerabilities, increasing the attack surface and exposing companies to potential threats and risks (Hess et al., 2016; Yilmaz & Yalman, 2016).

As emphasised in the literature, it is essential to increase resilience to cyber-attacks rather than focusing only on prevention. Companies need to be prepared for inevitable security incidents and can recover quickly (Bongiovanni, 2019). The human factor remains a crucial element of cyber security (Stewart & Jürjens, 2017). Therefore, employee training and awareness programmes are essential to minimise human errors and vulnerabilities (Yilmaz & Yalman, 2016; FireEye, 2015; Unit-Department, 2019).

The identification and mitigation of cyber threats require threat intelligence and advanced analytics (Allen, 2005; Lidster & Rahman, 2018; Whitman & Mattord, 2014). Real-time monitoring (Vejvodová, 2019), detection and response are essential to a robust security strategy. Compliance with cyber security regulations and standards is an ongoing challenge in DT (Vejvodová, 2019). The literature highlights that companies need to navigate a complex regulatory environment (Tiago et al., 2014).

Emerging technologies such as blockchain, quantum computing and 5G present opportunities and risks for DT (Barringer & Harrison, 2000; Wilkinson et al., 2004). Understanding their impact on cybersecurity is critical. Businesses are increasingly dependent on third-party vendors and partners (Wang et al.,

2013). Therefore, managing third-party risks is essential to cybersecurity, as their vulnerabilities can affect the organisation's security posture (Barlette et al., 2017). Executive engagement and involvement are critical to shaping a cybersecurity culture and ensuring digital transformation initiatives prioritise security from the outset.

2.10. The Nine Five Circle (NFC) Model

The NFC model is based on a rotation-driven approach to ensure reliability, efficiency, effectiveness, and consistency, using the pivot shown in Figure 3. The minimum number of rotations is five times each life cycle to stabilise the process. The rotation starts at the 9 o'clock, 12 o'clock, 3 o'clock, 5 o'clock, 6 o'clock and 7 o'clock positions. The cycle is then repeated after the fifth round. The critical variable is positioned at 9 o'clock, regardless of how many variables are involved, and the minimum number of rounds is five in each life cycle. This entire process is the foundation of NFC. The process of stabilisation is often referred to as the SDCA (Standardise-Do-Check-Act) cycle. This is a PDCA version, developed in the 1920s and popularised by Deming in the 1950s. It is also known as the Deming Cycle or Deming Wheel (Deming, 1982). According to Ishikawa (1985), failure to revise standards and regulations proves that no one is applying them seriously.

Each variable derived in the situational awareness phase is analysed and prioritised by comparing the impact and probability in each life cycle. Since information security and cybersecurity do not exist in a vacuum, their effectiveness and success depend on a combination of variables and their suitability to the implementation conditions. Knowledge strategy is derived from the organisation's competitive approach and describes the organisation's strategic plans for using knowledge to gain an advantage over competitors (Zack, 1999; Holsapple & Jones, 2006). In general, the overall goal of any cybersecurity programme is determined by its knowledge strategy.

The governance, risk, and compliance (GRC) department or facilitators define and determine the motivation behind the process and set guidelines that deal with the rules and regulations within the cybersecurity management process and between it and the rest of the organisation. The business environment in which the project is conducted and the organisation's chosen knowledge strategy are other external factors that prevent the proper creation of a cybersecurity plan. The business environment, corporate culture, level of ICT skills and resources available to the information security

policy plan to implement the information security policy are referred to as the corporate context (Doherty & Fulford, 2006; Sohrabi et al., 2016; Knapp et al., 2009; Kadam, 2007; Lucila, 2016).

Organisations that excel in cybersecurity have a clearly defined and well-planned approach to information security knowledge management (ISKM), according to research by Akhavan et al. (2006) and du Plessis (2007). The NFC framework uses information security and cybersecurity misperception to evaluate how well different aspects of an organisation's security policies align with contextual constraints and how effective remedial actions might be. ISKM involves educating staff about an organisation's information security policy and increasing staff awareness of security measures.

Facilitators are responsible for guiding the security strategy team through a defined activity sequence that maps the project's progress from initiation to completion. In this phase, measures and controls are defined, tested, implemented, and monitored. This integration phase includes process management (planning, training, testing), operational (process, procedures, protocols), tactical (evidence collection, triage, initial analysis), and practical and individual activities.

Effective risk management involves continuously identifying, assessing, and mitigating risks. It is a critical component of overall risk management, which includes devising and implementing strategies to reduce or transfer risks to an acceptable level (Silva et al., 2019). The NFC cybersecurity model provides a framework for implementing risk management at different levels, depending on the nature and objectives of the organisation (Sulistyowati et al., 2020). Rather than being a separate or isolated activity, the NFC ensures that risk management is integrated into the overall management process of an organisation (Malatji, 2023). This integration ensures that risk management becomes a standard practice that is consistently and successfully applied (Malatji, 2023) and becomes an integral part of the organisational culture.

2.10.1. Development of the NFC Model

2.10.1.1 Stage 1: Situational Awareness (SA)

Situational awareness is a process that helps decision-makers make intelligent cybersecurity decisions (Salmon et al., 2008). It facilitates the acquisition of relevant information across all business functions and the integration and sharing of this information for more thoughtful decision-making. Situational awareness is the capacity to identify environmental factors over a broad range of space and time, to understand their significance, and to predict how they will behave soon (Endsley, 1995). In recent years, the topic of SA has gained significant attention in the field of cyber security research. Technically, SA

refers to the process of compiling, compressing, and fusing data related to cyber security. The cognitive theoretical basis of Information Situational Awareness (ISA) is associated with this process. The specific notion of Cyber SA (CSA) was introduced in an edited volume by Jajodia et al. in 2009.

The situational awareness phase analyses and disseminates data regarding pertinent organisational variables' status, characteristics, and dynamics, such as cybersecurity posture, security culture, humans, assets, and processes (Salmon et al., 2017). At the individual level, situational awareness is the mental state resulting from the process in the ISA model (Endsley, 1995). It is the stage at which human efforts in collecting and using information are highlighted by establishing the meaning of things and occurrences. The more transparent this information is, the easier it is to predict and protect it through clearly defined security policies, up-to-date inventories, adequate access controls and detailed network diagrams (Kaber & Endsley, 1998). Adequate documentation of corporate information is needed (Salmon et al., 2009). Transparency and adequate documentation provide a reasonably exact depiction of the organisational context. This transparency is achieved through observations of users, processes, applications, known vulnerabilities, change management and usage patterns. This phase can be seen as the NFC gap analysis phase. Table 2 lists the significant variables identified in Papers 1 through 6 based on hypotheses and observations. These variables are then utilised in the integration phase.

Table.2 Variables that hinder cybersecurity progress.

Papers	Cybersecurity Critical Variables	Latent variables	Results achieved through "Method"
Paper 1	<ul style="list-style-type: none"> ● Data security ● Consumer trust 		Qualitative & Quantitative
Paper 2	<ul style="list-style-type: none"> ● Data security ● Consumer trust ● Privacy 		Quantitative & Quantitative
Paper 3	<ul style="list-style-type: none"> ● Security Misperception ● Application security training ● Application development ● Information security awareness ● Information security Misperception ● Investment in information security ● External and stakeholders' commitment 		Participatory, Observations & Interview
Paper 4	<ul style="list-style-type: none"> ● Security Misperception 		Participatory, Observations & Interview

	<ul style="list-style-type: none"> ● Evaluation of threat Vulnerability and Risk ● Cybersecurity Strategy ● Secure System Engineering ● Security Testing and Evaluation ● Protective Monitoring ● Strategic Advanced Threat Intelligence ● Incident Response and Remediation 	<ul style="list-style-type: none"> ● Communication ● Culture ● Trust ● Privacy ● Consultation 	
Paper 5	<ul style="list-style-type: none"> ● Lack of security interest ● Lack of security training and awareness ● Absence of compliance policy ● Lack of management directives 		Participatory, Observations & Interview
Paper 6	<ul style="list-style-type: none"> ● Security intelligence ● Cyber threat intelligence ● External partners ● Organisational commitment ● Information security misperception ● Information security investment 		Participatory, Observations & Interview

The data collected during the data collection and analysis phase is categorised to enable decision-makers to identify any difficulties associated with variables and other latent variables that threaten an asset (Jonathan, 2019; Moon et al., 2018). Situational awareness aims to understand the security situation within an organisation, which also helps create relevant and latent variables (Nazir & Han, 2022; Pahi, et al., 2017). Each variable is divided into its topology, while the latent variables are grouped, as shown in Figure 4 and Table 2 (Dillon et al., 1996). At this level, an effort is made to determine the optimum method for bringing about the desired change in the existing circumstances. The decision to take one course of action from a limited number of options leads to a resolution (McGuinness & Foy, 2000). The collected and latent variables are then forwarded to the integration control for further processing, including cybersecurity programmes and implementations. A risk-based validation process is applied to both variables and latent variables to maintain the data accuracy (Moon

et al., 2018). This involves filtering out any unusable data and cleaning up the remaining data. A risk analysis is then performed to identify any problematic variables that may pose a security threat to the organisation (Stewart & Jürjens, 2017).

a. Assets Protection

Organisations must protect their information systems and resources from cyber threats regardless of size or location. This includes classifying, prioritising, and protecting information systems based on their level of risk, criticality, and legal implications (Yu et al., 2022; Sofi, 2016; Barua et al., 2022).

Ulven and Wangen (2021) provided an overview of mission-critical assets and common cybersecurity vulnerabilities, highlighting the general threat model and everyday threats. Conversely, Chen and Fiscus (2018) focused on the hospitality industry, identifying several cybersecurity issues by analysing 76 security incidents from the Privacy Rights Clearinghouse database, which are listed in Supplementary Table 1. In addition, eight studies were conducted to determine the costs of data breaches. For instance, Eling and Jung (2018) studied data breaches over several decades and found an asymmetric dependence of monthly losses by breach type and industry.

Several layers of DT are critical as it combines various communication technologies that enable IoT devices to communicate with each other. Several methods of communication have been studied, including those by Yu et al. (2022), Sofi (2016), and Barua et al. (2022). Cybersecurity measures must be implemented at every stage of the DT environment lifecycle to protect this infrastructure from unauthorised access, modification, or loss (Rouhani et al., 2021). The action plan should consider technical security measures, such as firewalls and anti-virus protection, as well as user protection, such as proper authentication and access restrictions. Logical security measures, such as encryption and secure application programming, should also be considered.

Prioritising measures such as hardening information systems, security awareness training, and appropriate incident protection is crucial. Security leaders should understand the significance of business functions supported by information systems to make informed decisions on priority setting. Organisations must prioritise after determining what needs to be protected, why, and from what. As shown in Table 3, the derived variables and the latent variables serve to protect organisational IS.

b. Information security policy (ISP) and governance

Effective ISP and governance are crucial for any business to protect its assets and reputation. In order to achieve this, top management must be committed to implementing policies and procedures, as

highlighted by Allen & Westby (2007), Schinagl & Shahim (2020), and Von Solms (2001). Previously, management viewed information security as a technical issue to be handled solely by IT (Posthumus & Von Solms, 2004a; Von Solms, 2001). However, Allen and Westby (2007) emphasised the importance of distributing information security responsibilities across various organisation departments. This requires cross-organisational interaction, collaboration, and commitment. Ensuring the long-term sustainability and protection of the organisation requires information security to be considered as a strategic governance issue (Allen, 2005; Lidster & Rahman, 2018; Whitman & Mattord, 2014).

Management needs to recognise the significance of information security and provide appropriate directives based on several factors, such as the company's strategic vision, legal and regulatory requirements, the role of IT, its alignment with corporate strategy, and competitiveness (Von Solms, 2006). Hence, organisations must implement an Information Security Policy Architecture (ISPA) that outlines all information security-related policies in a hierarchical structure. This approach will help organisations strategically and tactically understand their ISP and how they are interrelated (Bacik, 2005). The foundation of IS protection is good policy and governance (Von Solms, 2006; Allen & Westby, 2007; Schinagl & Shahim, 2020). The measures considered security challenges (see Table 2) depend on the goals and requirements of the organisation. The stricter the standards, the easier it is to detect a breach and prevent it from happening in the first place. However, the policies and requirements must be made available to security professionals for detection and prevention to be effective (Allen, 2005; Lidster & Rahman, 2018; Whitman & Mattord, 2014).

The classification of IS, their use and who is allowed to use them can be used to prevent security breaches or to act quickly in the event of a security breach (Stewart, 2022). Management is the decision-making about business processes and procedures. Governance refers to a series of principles and values governing an organisation's business approach. In contrast, information security governance refers to principles and visions governing the organisation's process to establish an effective, efficient, and consistent cybersecurity system. The ISO/IEC 27014:2020 offers organisations guidance for evaluating, managing, controlling, and communicating processes related to information security within an organisation, along with ideas, goals and processes related to information security (Allen, 2005; Lidster & Rahman, 2018).

2.10.1.2 Stage 2: Integration Control

During the integration phase, the cybersecurity program aims to establish governance objectives and control activities by measuring the relationship between critical and latent variables (Kabanda et al.,

2018). The NFC model comes in handy here by accounting for measurement errors by representing unobserved variables in these relationships (Stewart, 2022). The goal is continually monitoring and measuring the entire process to ensure a reliable and predictable outcome for information security risk management (ISRM). This whole process is accomplished by breaking down the complexity of the process into different latent variables and interrelated variables, which are then integrated back into one view to provide a comprehensive understanding of the process (Islam et al., 2017). Widely accepted risk management standards, such as ISO 31000, provide guidelines for risk management activities and consider it an integral part of overall organisational processes, including strategic planning and management processes (ISO). Another recognized risk management technique is IEC 31010 (GOST, 2009).

Managers are responsible for establishing unambiguous and effective risk management policies that align with the company's mission and objectives as part of their governance duties. At every level of the organisation, leaders should express their risk appetite and tolerance expectations. These principles form the basis of the business strategy, ensuring that the various risks are managed at an acceptable level. As the risk landscape evolves, for example, due to technological changes and the environment, business leaders should consistently review and adjust their risk strategy. If a company is subject to external regulation, it may receive specific guidance on updated federal laws and guidelines that need to be considered when assessing acceptable risk (Barlette et al., 2017).

Effective decision-making in information risk management involves the participation of owners and managers (Bayaga et al., 2017). This highlights the crucial role that leadership plays in mitigating cybersecurity threats. Usually, managers are the ultimate decision-makers, especially when defining the organisation's information security strategies (Barlette et al., 2017). Kabanda et al. (2018) state that top-level executives, including CEOs, are directly responsible for cybersecurity implementation decisions. Previous studies on organisations have revealed that executives often depend on experts and social networks when making decisions (Barlette et al., 2017). Therefore, professionals and experts can be an essential part of and aid the decision-making process within a company.

Organisations responsible for critical infrastructure can use the NIST framework with existing frameworks to systematically identify, measure, assess, and leverage cybersecurity risks. The framework can be used as a basis for a new cybersecurity program or to improve an existing one (NIST, 2011). The results obtained from the framework are used for the ongoing operation of the system, which includes regular reassessment to ensure that cybersecurity requirements are met (Purdy, 2009).

One risk management approach, as outlined by Islam (2017), places a strong emphasis on identifying specific organisational goals. Risks are seen as obstacles to these goals and, therefore, assessed based on which goals they could impede. The approach is applicable in various domains, including DT projects such as cloud computing and software development.

Cybersecurity programme

Organisational knowledge transfer has been extensively studied by various authors such as Fiol and Lyles (1985), Huber (1991), Easterby-Smith & Lyles (2012), and Argote (2013). Argote (2013) defines it as a transformation within an organisation's knowledge resulting from experience. Fiol and Lyles (1985) describe it as incorporating new knowledge into an organisation's actions, while Argote and Ophir (2017) recognise it as a process of making changes resulting from experience. A significant amount of research is available on general organisational learning, focusing on using knowledge to enhance organisational productivity or competitiveness (Senge, 2010). Building a cybersecurity programme is part of the first phase of the cybersecurity management lifecycle. The steps involve; (i) Developing a corporate justification for cybersecurity, (ii) management support and funding, (iii) establishing a cybersecurity team, (iv) defining the scope of cybersecurity management, (v) establishing policies and procedures, and (vi) identifying and classifying assets (e.g., Herath and Rao, 2009; Ifinedo, 2012; Crossler et al., 2013).

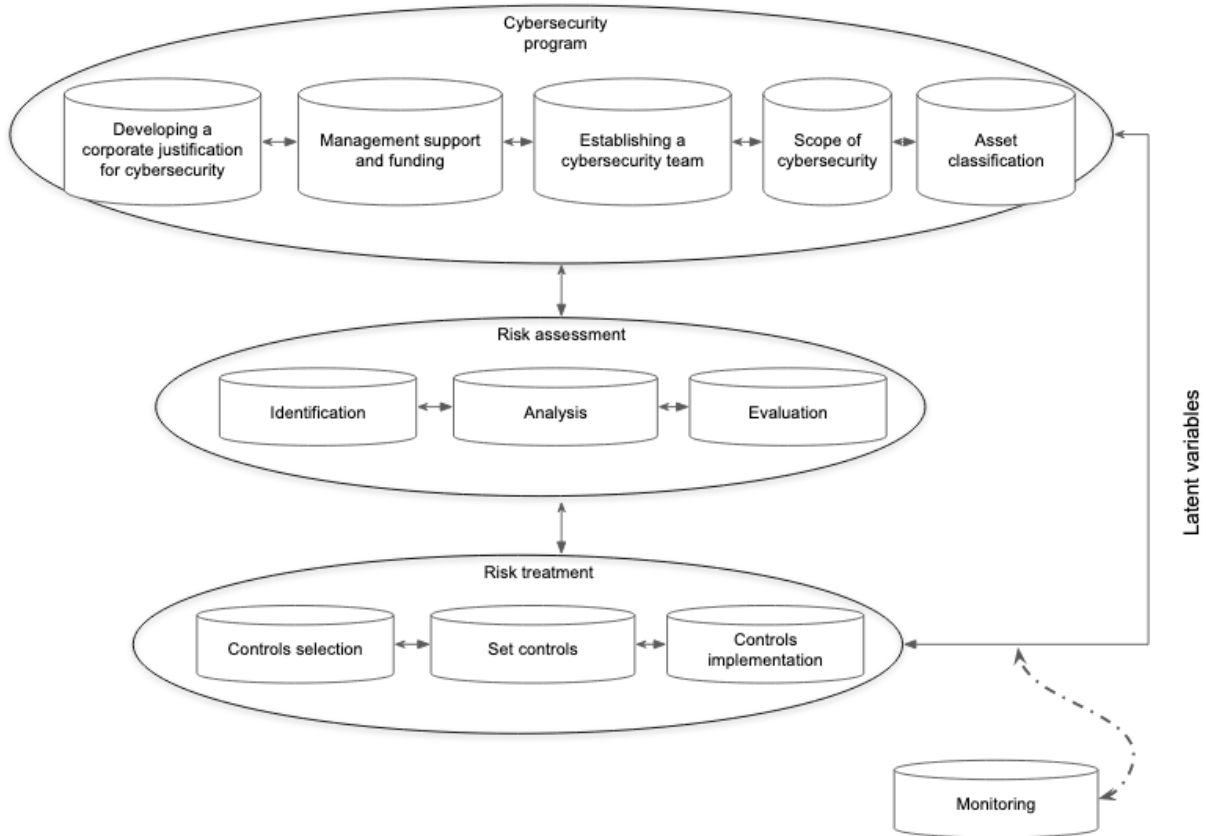


Fig. 4 NFC situational awareness process

As shown in Figure 4, the next step after the cybersecurity program is to perform risk assessment followed by risk treatment (e.g. Cheminod et al., 2013; Leith and Piper, 2013; Kaplan and Garrick, 1981; Chittester and Haines, 2004).

Organisations face difficulties in obtaining a comprehensive view of their cyber assets when using multiple technologies because each tool has its definitions of assets (Barlette et al., 2017). The advent of cloud computing and digital transformation has drastically changed how organisations are managed and protected, resulting in the use of various security tools to safeguard their cyber assets (Bayaga et al., 2017).

Another key factor is threat classification where each threat is classified based on their criticality (Barlette et al., 2017). The classification of each asset determines the complexity of the controls that must be put in place to protect them. Per ISO27001, each cybersecurity attribute, i.e., confidentiality, integrity, and availability, must be considered independently in the three matrix impact categories of low, medium, high, significant, and severe. as shown in Table 3. Classifying risks helps to identify and classify security threats, which enables the assessment of their impact and the development of

prevention or mitigation measures (Bompard et al., 2013; Tang et al., 2012; Farahmand, 2005). The threats in this research are represented by the variables listed in Table 2, which were discovered during the situational awareness phase.

Risk Assessment

Risk identification involves identifying and categorising potential risks to assets and business operations that may negatively affect performance, harm, or reputation (Islam et al., 2017; ISO 31000:2009; Cheminod et al., 2013). The main challenge in this stage is ensuring that the analysis is comprehensive and covers all significant aspects (NIST, 2011). The fundamental strategy to overcome this obstacle is establishing and maintaining distinct expertise of threats. The list should be updated regularly from relevant sources, such as the Computer Emergency Response Team (CERT) website, the Information Sharing and Analysis Centre (ISAC), the anti-malware provider's website and databases, in addition to regular exchanges of information with both operators and other actors (Bayaga et al., 2017). It is essential to regularly update the repository from relevant sources, such as the Computer Emergency Response Team (CERT) website, the Information Sharing and Analysis Centre (ISAC), the anti-malware provider's website and databases, and by regularly exchanging information with operators and other stakeholders (Cheminod et al., 2013; Chittester and Haimes, 2004).

After the identification of potential risks, the next step is risk evaluation. This step thoroughly evaluates the risks and unforeseen cases based on the risk base. A summary judgement is made about these risks. The evaluation must distinguish between the evidence required to support an assertion and the actual burden of proof for a particular decision. It should also consider the decision maker's values. However, evaluation is quite complicated and requires the input of safety experts. Decision-makers must not rely solely on risk evaluation but also integrate risk information with other data sources and topics.

It is essential to record all identified potential risks in a risk registry and regularly review them to inform management about cybersecurity threats.

Risk Treatment

Although various risk management principles and strategies have been published to address risks, decision-makers must know their organisation's risk management strategies and process structure. Risk treatment strategies are an essential component of the risk management process. It includes three strategies - risk-informed, preventive, and discursive (Renn, 2008). The appropriate strategy is often a

mixture of these three. The risk-informed strategy primarily focuses on accepting, avoiding, transferring, or mitigating risks using absolute or relative risk assessments. The preventive strategy aims to reduce risks, enhance system resilience, and improve emergency response capabilities.

Organisations must be able to identify potential risks and any factors that may cause significant harm. Effective risk management relies on these principles to address uncertainties, potential risks, and unexpected exposures. The digressive approach builds trust to reduce security misperceptions among decision-makers (Renn, 2008).

The process structure of risk management can be divided into several stages, as outlined by researchers such as Aven (2015a) and Meyer and Reniers (2013). These stages include establishing risk content, identifying risks, events, causes, and consequences, decision-making, evaluation of risk, and risk treatment.

Risk assessments are crucial for making informed decisions. They help evaluate options and accept activities and implement risk-reduction strategies during decision-making. Decision analysis tools such as cost-benefit, cost-effectiveness, and multi-attribute analyses can supplement the generation of risk information. These methods use systematic approaches to organise the advantages and disadvantages of a decision alternative, which vary depending on how explicitly comparable the problem factors are (Gilboa and Marinacci, 2013). Despite the tool employed, management must consistently review and use discretion beyond the analysis's findings. This is done to consider the knowledge, or lack thereof, on which the assessments are predicated, as well as factors that the analysis should have covered. Risk management and policy are closely linked principles that guide decision-making and enable desirable outcomes (Althaus et al., 2007).

2.10.1.3. Stage 3: Gap Closure

During the gap closure phase, security is established based on cybersecurity guidelines (Dempsey et al., 2011). This phase involves a comprehensive strategy that covers all aspects of information and cyber security, including procedures, documentation, roles, tasks, and personnel within the defined scope. A report on security control level gaps provides a thorough analysis of the current security state and a plan to address any gaps. The plan includes specific roles, tasks, timeframes, and estimated effort. Regular monitoring of performance and risk indicators helps to reduce the organisation's risk exposure (Vejvodová, 2019). Monitoring is to consistently manage cybersecurity, assess its effectiveness, adherence to security standards and remain aware of any changes in the organisation's internal and external environment that may impact its risk level.

The NFC situational awareness is constantly monitored and improved to enhance the overall security of the process (Khallaf & Majdalawieh, 2012). Additionally, a better understanding of the control of security processes during integration helps to increase employees' situational awareness while working in the organisation's IT infrastructure (Ashenden, 2008; Khallaf & Majdalawieh, 2012). Therefore, implementing the NFC process is a recursive process. As NFC is a recursive process, the exchange of security-related information between stakeholders and DT's security processes is interdependent. It is crucial to involve associated requirements during this communication to ensure proper input and output (Khallaf & Majdalawieh, 2012). Therefore, collecting data and defining the appropriate variables play a fundamental role in calculating metrics for the security control process. During the situational awareness phase, gathering relevant information and taking appropriate actions based on the findings is crucial. The collected data must then be evaluated for effectiveness to achieve continuous process improvement (Madsen, 2013).

In addition, adherence to ISPs during the implementation phase is critical to ensure that all employees have the same organisational vision and goals. Although adherence to ISPs is cited in the literature as a challenge for different organisations (Ashenden, 2008), well-established and informed ISPs are essential for technological improvements that can help different industries. Dawson (2017) defines cybersecurity frameworks as policies and procedures that help to implement and maintain information security controls continuously. These frameworks amalgamate various elements such as training, policies, and technologies and can adapt to existing requirements while controlling new ones. Integrating a cybersecurity framework can facilitate business and cybersecurity risk management by validating them with top management. This ensures an updated understanding of cybersecurity risks (Cockcroft, 2020; Ferruzola et al., 2019).

In case of inaccurate results, the system searches for potential causes that led to the inaccuracy and identifies the fundamental issues, including improper connection of components defined in the NFC. Once the root cause is identified, the system initiates an appropriate response. For instance, if a lack of security information sharing is identified as a problem, managers are notified of employee negligence during cyber-attacks (Madsen, 2013). Moreover, security-related information helps establish predefined metrics for the NFC system. By feeding well-defined components into the NFC system, the security areas of the system can be improved, and potential vulnerabilities in the DT can be better managed. According to Lambrinouidakis et al. (2022), information security management frameworks enable organisations to incorporate or merge different processes within their context to meet the

requirements of their operational environment. These frameworks provide specific taxonomies for categorising risks, which help organisations manage, avoid, share, or accept risks as necessary. ISO/IEC 27001:2022 guidance emphasises that control selection must be based on results and conclusions of risk analysis (Lopes et al., 2019).

Tatiara et al. (2018) studied the obstacles to implementing ISMS. They concluded that successful implementation requires the involvement of all stakeholders. To achieve this, they recommend taking specific actions such as including top management in the process, communicating employee policies regularly, conducting periodic reviews of information security management systems (ISMS) implementation, informing employees about any improvements, and regularly communicating roles, responsibilities, and authorities related to ISMS to employees. The authors also suggest developing work programs for implementing information security systems and distributing them to employees.

2.11. NFC Model validation

2.11.1. Observation

During the observation phase, a systematic approach is used to focus on various activities that highlight the differences in the NFC model. To achieve this, researchers must participate in and observe these activities for a significant amount of time. Researchers can articulate their findings through engagement with participants and improve the current development process. Building trust is crucial at this stage to encourage participants to share openly (Taylor & Bogdan, 1984; Merriam, 1998; DeWalt & DeWalt, 2002; Wolcott, 2001; Lincoln & Guba, 1994).

2.11.2. Evaluation

In order to create precise evaluation maps, it is vital to eliminate preconceived notions or biases. The mapping method can be based on the approach of Kutsche (1998). A detailed physical map of the organisation's environment should be made, including as much detail as possible. The organisation should be studied several times to assess how the findings and recommendations can be used in different application development projects. To practise cultural relativism, researchers must refrain from making value judgements and instead use relevant adjectives to meaningfully describe the distinct aspects of the environment (Schensul et al., 1999). Only one of the five senses, vision, is used in this mapping procedure. This observation phase should last at least four months. Any positive feedback and summary constructs that underpin the lessons learned by an organisation can be identified and integrated into the following context using the following constructs:

- A clearly defined and focused application security strategy.
- Strict alignment between the application security strategy and the organisation.
- A thorough consideration of the business and organisational context.

2.11.3. Reliability and Validity at Post-fieldwork Stage

2.11.3.a. Reliability

Construct reliability and coefficient alpha were utilised to assess reliability in this thesis. The coefficient alpha was determined using SPSS, and values above 0.5 were considered satisfactory, although there is no universally agreed-upon threshold (Hair et al., 2006; Kline, 2005). If the coefficient alpha for a construct exceeded this threshold, it was deemed reliable. To determine the reliability of each construct, standardised item loadings and error measures were obtained from the congeneric models using data from AMOS (Byrne, 2001; Kline, 2005).

2.11.3.b. Validity

The degree of correlation between measurements of the same construct is measured by convergent validity (Churchill, 1979). The item loadings were acceptable when using single-factor congeneric models, as they all exceeded the threshold of 0.7. (Steenkamp and van Trijp, 1991). The variance collected was also used to calculate convergent validity. This is a measurement of the construct's variance compared to the variance lost due to measurement error (Fornell & Larcker, 1981). The section on the corresponding papers contains the data used to calculate the extracted variance. All constructs show convergent validity as the extracted variance equals or exceeds the lower bound 0.7. Discriminant validity assesses the uniqueness and novelty of each measure as opposed to convergent validity (Churchill, 1979; Meyer & Page, 2000). Using a commonly used technique by Fornell and Larcker (1981), discriminant validity was assessed by comparing the variance derived from each construct with the square of the highest correlation each factor has with other factors (Ramani & Kumar, 2008; Rokkan et al., 2003; Straub, 1989). If the square of the greatest common variance of the factors were greater than 0.500, all factors would exhibit discriminant validity.

2.12. NFC Summary

The development and analysis of the NFC cybersecurity model represent a significant stride forward in addressing the escalating challenges posed by the DT landscape (Silva et al., 2019). As organisations continue to embrace innovative technologies to remain competitive, the need for a robust and adaptable cybersecurity approach has never been more apparent. This model, informed by theoretical

underpinnings and practical insights, offers a comprehensive solution to enhance the security of DT initiatives (Sulistyowati et al., 2020).

One of the key takeaways from this research is the imperative of a holistic approach to cybersecurity (Perkin & Abraham, 2017). The NFC model's multifaceted components, including (i) security misperception, (ii) threat vulnerability and risk assessment, (iii) cybersecurity strategy, (iv) development of secure information systems, (v) security audit and assessment, (vi) protection monitoring, (vii) strategic advanced threat analysis, (viii) incident response and remediation, (ix) managers and stakeholders involvement, (x) information security and cybersecurity investments, (xi) information security policies, (xii) application security policies, (xiii) information security facilitators, (xiv) security training, (xv) commitment, and (xvi) external partners, provide organisations with a well-rounded strategy to safeguard their digital transformation endeavours. The model's adaptability, informed by emerging technologies and real-time threat intelligence, ensures that it remains effective in ever-evolving cyber threats (Perkin & Abraham, 2017).

Moreover, the NFC model contributes to the ongoing shift in cybersecurity philosophy from focusing solely on prevention to equally prioritising resilience and response (Dawson, 2017). In an era of advanced persistent threats, the capacity to recover swiftly from incidents takes centre stage in ensuring business continuity (Holgate et al., 2015; Mujinga et al., 2012; Paja et al., 2017).

The practical contributions of the NFC model are evident in its capacity to streamline security operations, reduce vulnerabilities, and enhance risk management (Perkin & Abraham, 2017). Organisations can ensure employees are trained in cybersecurity, creating a more secure digital environment (e.g., D'Arcy et al., 2009; Schneier, 2011; Crossler et al., 2013). Compliance remains a significant challenge in the DT landscape (Stewart, 2022). The model is well-equipped to assist organisations in navigating the intricate regulatory environment. The model's compliance features help ensure alignment with industry-specific standards and regulations, mitigating the risk of non-compliance and its associated penalties (Wessel et al., 2020).

In conclusion, the NFC Cybersecurity model offers a dynamic and adaptable solution to the cybersecurity challenges associated with DT (D'Arcy et al., 2009; Schneier, 2011; Crossler et al., 2013). It provides organisations with the tools, strategies, and resilience needed to protect their digital assets, foster trust among stakeholders, and ensure the successful implementation of transformative digital initiatives (Bekkhush, 2016; Bharadwaj et al., 2013; Matt et al., 2015). As the digital landscape continues

to evolve, the NFC model is a pivotal asset in fortifying cybersecurity in this era of innovation and change. Organisations must consider its adoption a cornerstone in their strategy for secure and successful DT (Holgate et al., 2015; Mujinga et al., 2012; Paja et al., 2017).

2.13. References

- A. Bayaga, S. Floerday, and L. Cilliers, "IT Risk and Chaos Theory: Effect on the performance of South African SMEs," in *WMSCI 2017 - 21st World Multi-Conference Syst. Cybern. Informatics, Proc.*, vol. 2, no. 5, 2017, pp. 48–53.
- A. Bayaga, S. Floerday, and L. Cilliers, "IT Risk and Chaos Theory: Effect on the performance of South African SMEs," in *WMSCI 2017 - 21st World Multi-Conference Syst. Cybern. Informatics, Proc.*, vol. 2, no. 5, 2017, pp. 48–53.
- Alhabeeb, M., Almuhaideb, A., Le, P., & Srinivasan, B. (2010). Information Security Threats Classification Pyramid. 24th IEEE International Conference on Advanced Information Networking and Applications Workshops. doi:10.1109/WAINA.2010.39
- Allen, J. (2005). Governing for enterprise security. Carnegie Mellon University/Software Engineering Institute Technical Note CMU/SEI-2005-TN-023. WWW document viewed 1/09/2019 from <http://www.cert.org/archive/pdf/05tn023.pdf>.
- Allen J, Westby J. Governing for Enterprise Security (GES) Implementation Guide. USA: Carnegie Mellon University, Software Engineering Institute, CERT; 2007.
- Althaus, C., Bridgman, P., & Davis, G. (2007). The Australian policy guidance (4th ed.). Sydney: Allen & Unwin.
- Angelini, M, N. Prigent, and G. Santucci. Percival: proactive and reactive attack and response assessment for cyber incidents using visual analytics. In 2015 IEEE Symposium on Visualization for Cyber Security (VizSec), pp. 1–8. IEEE, 2015.
- Applegate, D. S., & Stavrou, A. (2013). Towards a cyber conflict taxonomy. 5th International Conference on Cyber Conflict. IEEE Xplore Digital Library.
- Argote, L., 2013. Organizational Learning, 2nd ed. Springer US, Boston, MA doi:10. 1007/978- 1- 4614- 5251- 5

Argote, L., 2013. *Organizational Learning*, 2nd ed. Springer US, Boston, MA doi:10. 1007/978- 1- 4614- 5251- 5

Argote, L., Ophir, R., 2017. Intraorganizational learning. In: in *The Blackwell Companion to Organizations*. Blackwell Publishing Ltd, Oxford, UK, pp. 181–207. doi:10.1002/9781405164061.ch8.

Argote, L., Ophir, R., 2017. Intraorganizational learning. In: in *The Blackwell Companion to Organizations*. Blackwell Publishing Ltd, Oxford, UK, pp. 181–207. doi:10.1002/9781405164061.ch8.

Arthur, K., & Olivier, M. (2017). Applying The Biba Integrity Model to Evidence Management. IFIP International Conference on Digital Forensics (pp. 1-15). Pretoria: National Centre for Forensic Science.

Ashenden, D. (2008). Information Security management: A human challenge?. *Information Security Technical Report*, 13(4), 195-201. <https://doi.org/10.1016/j.istr.2008.10.006>

Aven, T. (2015a). *Risk analysis* (2nd ed.). Chichester: Wiley.

B. McGuinness and J. L. Foy. A subjective measure of SA: The crew awareness rating scale (cars). In *Proceedings of the first human performance, situation awareness, and automation conference*, Savannah, Georgia, USA, October 2000.

Bacik S. *Building an effective information security policy architecture*. CRC Press, Taylor & Francis Group: Boca Raton, 2008.

Barua, A.; Al Alamin, M.A.; Hossain, M.S.; Hossain, E. Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey. *IEEE Open J. Commun. Soc.* 2022, 3, 251–281.

Baskerville, R., 1988. *Designing Information Systems Security*. John Wiley & Sons, New York.

Baskerville, R. (1999). Investigating Information Systems with Action Research. *Communications of the Association for Information Systems*, 2, pp-pp. <https://doi.org/10.17705/1CAIS.00219>

Bekkhush, R. (2016). Do KPIs used by CIOs decelerate digital business transformation? The case of ITIL. Paper presented at the Digital Innovation, Technology, and Strategy Conference, Dublin, Ireland. In the *Proceedings of DIGIT 2016*. <https://aisel.aisnet.org/digit2016/16>

- Bell, D. E. (1973). *Secure Computer Systems: Mathematical Foundations*, Bedford. Bedford, MA: MITRE.
- Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. *MIS Quarterly*, 37(2),471-482.
- Biba, K. J. (1977). Integrity considerations for secure computer systems. Bedford, Massachusetts: ESD-TR.
- Bodeau, D., McCollum, C., Fox, D., 2018. *Cyber Threat Modeling: Survey, Assessment, and Representative Framework*. The Homeland Security Systems Engineering and Development Institute, The MITRE Corporation.
- Bompard, E., Huang, T., Wu, Y., & Cremenescu, M. (2013). Classification and trend analysis of threatsorigins to the security of power systems. *Electrical Power and Energy Systems*, 50, 50–64. doi:10.1016/j.ijepes.2013.02.008
- Brewer, D. F., & Nash, M. J. (1989). The Chinese wall security policy. *IEEE Symposium on Security and Privacy*, (pp. 1-13). Oakland, CA.
- Byrne, B. (2001) *Structural Equation Modeling With AMOS: Basic Concepts, Applications, and Programming*, New Jersey, Lawrence Erlbraum Associates, Inc., Publishers.
- Cheminod M, Durante L, Valenzano A. Review of security issues in industrial networks. *IEEE Trans Industr Inform* 2013;9(1):277–93.
- Chen, H.S., and J. Fiscus. 2018. The inhospitable vulnerability: A need for cybersecurity risk assessment in the hospitality industry. *Journal of Hospitality and Tourism Technology* 9 (2): 223–234. <https://doi.org/10.1108/JHTT-07-2017-0044>.
- Chen, S.P. and Redar, J.M. (2014),“Ageing workforce knowledge management and transactional andtransformational leadership: a socio-technical systems framework and a norwegian case study”,*International Journal of Business and Social Science*, Vol. 5 No. 5, pp. 11-
- Cheng, E.C., 2000. An object-oriented organizational model to support dynamic role-based access control in electronic commerce. *Decision Support Systems* 29 (4), 357–369.
- Chittester C, Haimes YY. Risks of terrorism to information technology and to critical interdependent infrastructures. *J Homel Secur Emerg Manag* 2004;1(4):article 402.

- Chu, M, K. Ingols, R. Lippmann, S. Webster, and S. Boyer. Visualizing attack graphs, reachability, and trust relationships with navigator. In Proceedings of the Seventh International Symposium on Visualization for Cyber Security (VizSec), pp. 22–33, 2010
- Churchill, G. A. (1979) 'A Paradigm for Developing Better Measures of Marketing Constructs'. *Journal of Marketing Research*, Vol.16 No.1, pp.64-73
- Clark, D. D., & Wilson, D. R. (1987). A Comparison of Commercial and Military Computer Security Policies. Proceedings of the 1987 IEEE Symposium on Research in Security and Privacy (pp. 184–193). Oakland, CA: IEEE Press.
- Cockcroft, S. What is the nist framework. *ITNOW* **2020**, 62, 48–49. [Google Scholar] [CrossRef]
- Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future Directions for Behavioral Information Security Research," *Computers & Security* (32:2013), pp. 90- 101.
- Davis, M.C., Challenger, R., Jayewardene, D.N.W. and Clegg, C.W. (2014),“Advancing socio-technical systems thinking: a call for bravery”,*Applied Ergonomics*, Vol. 45 No. 2, pp. 171-180
- Dawson, M. Hyper-connectivity: Intricacies of national and international cyber securities. In PQDT—Glob; London Metropolitan University: London, UK, 2017.
- Dempsey, K., Chawla, N.S., Johnson, A., Johnston, R., Jones, A.C., Orebaugh, A., Scholl, M., Stine, K.: NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Tech. rep. (2011)
- Disterer, G. (2013) ISO/IEC 27000, 27001 and 27002 for information security management. *J Inform Security* 4(2):92–100
- Easterby-Smith, M., Lyles, M.A., 2012. *Handbook of Organizational Learning and Knowledge Management*, 2nd ed. John Wiley & Sons Ltd, Chichester Accessed: Feb. October, 2023. Available: [PDF] nibmehub.com.
- Easterby-Smith, M., Lyles, M.A., 2012. *Handbook of Organizational Learning and Knowledge Management*, 2nd ed. John Wiley & Sons Ltd, Chichester Accessed: Feb. October, 2023. Available: [PDF] nibmehub.com.

- Eling, M., and K. Jung. 2018. Copula approaches for modeling cross-sectional dependence of data breach losses. *Insurance Mathematics & Economics* 82: 167–180. <https://doi.org/10.1016/j.insma.2018.07.003>.
- Ellström, D., Holtström, J., Berg, E., & Josefsson, C. (2022). Dynamic capabilities for digital transformation. *Journal of Strategy and Management*, 15, 272–286.
- Emery, F.E. (1982), "Sociotechnical foundations for a new social order?", *Human Relations*, Vol. 35 No. 12, pp. 1095-1123. No
- Endsley, M.R., 1995. Toward a theory of situation awareness in dynamic systems. *Hum. Factors* 37 (1), 32–64.
- Farahmand, F. Navathe, S. B. Sharp, G.P. & Enslow, P. H. (2005). A Management Perspective on Risk of Security Threats to Information Systems. *Information Technology and Management Archive*, 6, 202-225.
- Felderer M et al (2014) Evolution of security engineering artifacts: a state of the art survey. *Int J Secur Softw Eng* 5:48–98
- Ferreira, A., Huynen, J., Koenig, V., and Lenzini, G. 2014. "A Conceptual Framework to Study Socio-Technical Security," in *International Conference on Human Aspects of Information Security, Privacy, and Trust*, Crete, Greece, 22-27 June, pp. 318-329.
- Ferreira, Ana & Huynen, Jean-Louis & Koenig, Vincent & Lenzini, Gabriele. (2014). A Conceptual Framework to Study Socio-Technical Security. *Lecture Notes in Computer Science*. 10.1007/978-3-319-07620-1_28.
- Ferruzola Gómez, E.; Duchimaza, S.J.; Ramos Holguín, J.; Alejandro Lindao, M. Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología MAGERIT. *Rev. Científica Tecnológica UPSE* **2019**, 6, 34–41. [Google Scholar] [CrossRef]
- Fiol, C.M., Lyles, M.A., 1985. Organizational Learning. *Source Acad. Manag. Rev.* 10 (4), 803–813.. Available <https://www.jstor.org/stable/258048?seq=1&cid=pdf>
- Fiol, C.M., Lyles, M.A., 1985. Organizational Learning. *Source Acad. Manag. Rev.* 10 (4), 803–813.. Available <https://www.jstor.org/stable/258048?seq=1&cid=pdf>

- Fornell, C. & Larcker, D. F. (1981) 'Evaluating Structural Equation Models with Unobservable Variables and Measurement Error'. *Journal of Marketing Research*, Vol.18 No.1, pp.39-50.
- Furnell, S. 2005. "Why Users Cannot Use Security," *Computers & Security* (24:4), pp. 274-279.
- Gilboa, I., & Marinacci, M. (2013). Ambiguity and the Bayesian paradigm. In D. Acemoglu, M. Arellano, & E. Dekel (Eds.), *Advances in economics and econometrics: Theory and applications*. Cambridge: Cambridge University Press.
- GOST-R. Risk Management. Risk Assessment Methods; ISO/IEC 31010-2011; International Organization for Standardization: Geneva, Switzerland, 2009.
- Hess, T., Matt, C., Benlian, A., & Wiesböck, F. (2016). Options for formulating a digital transformation strategy. *MIS Quarterly Executive*, 15(2).
<https://aisel.aisnet.org/misqe/vol15/iss2/6>
- Hong, J., Kim, D., 2016. Assessing the effectiveness of moving target defenses using security models. *IEEE Trans. Dependable Secure Comput.* 13 (2), 163–177,
<https://doi.org/10.1109/TDSC.2015.2443790>.
- Hong, J.B., Kim, D.S., 2016. Towards scalable security analysis using multi-layered security models. *J. Netw. Comput. Appl.* 75, 156–168, <https://doi.org/10.1016/j.jnca.2016.08.024>.
- Hong, J.B., Kim, D.S., Chung, C.-J., Huang, D., 2017. A survey on the usability and practical applications of graphical security models. *Computer Science Review* 26, 1–16,
<https://doi.org/10.1016/j.cosrev.2017.09.001>.
- Huber, G.P., 1991. Organizational learning: the contributing processes and the literatures. *Organ. Sci.* 2 (1), 88–115. Available <https://www.jstor.org/stable/2634941>
- Huber, G.P., 1991. Organizational learning: the contributing processes and the literatures. *Organ. Sci.* 2 (1), 88–115. Available <https://www.jstor.org/stable/2634941>
- Humphreys, E (2011) Information security management system standards. *Datenschutz und Datensicherheit* 35(1):7–11
- Islam, S.; Fenz, S.; Weippl, E.; Mouratidis, H. A Risk Management Framework for Cloud Migration Decision Support. *J. Risk Financial Manag.* 2017, 10, 10

Islam, S.; Fenz, S.; Weippl, E.; Mouratidis, H. A Risk Management Framework for Cloud Migration Decision Support. *J. Risk Financial Manag.* 2017, 10, 10

ISO/IEC: ISO/IEC 27001:2013: Information technology – Security techniques – Information Security management systems – Requirements (2013). URL
<http://shop.bsigroup.com/ProductDetail/?pid=000000000030313534>

ISO/IEC: ISO/IEC 27005:2011: Information technology – Security techniques – Information Security risk management. Tech. rep., ISO/IEC (2011)

ISO/IEC. 27000:2018, “Information technology—Security techniques—Information security management systems—Overview and vocabulary”, 2018.

ISO/IEC. 27001:2013, “International standard ISO/IEC Information technology—Security techniques—Information security management systems—Requirements”, vol. 2013, 2013.

ISO/IEC. 27002:2013, “Information technology—Security techniques—Code of practice for Information security controls”, 2013.

ISO/IEC. 27017:2015, “Information technology—Security techniques—Code of practice for information security controls based on ISO/IEC 27002 for cloud services”, 2015.

ISO/IEC 27032:2012 (E) information technology e security techniques e guidelines for Cyber Security, Geneva, Switzerland:ISO/IEC, 2012.

ISO. Risk Management—Principles and Guidelines; ISO 31000:2009; International Organization for Standardization: Geneva, Switzerland, 2009.

ISO. Risk Management—Principles and Guidelines; ISO 31000:2009; International Organization for Standardization: Geneva, Switzerland, 2009.

Jagadamba G, Sharmila S, Gouda T (2014) A secured authentication system using an effective keystroke dynamic. In: *Emerging research in electronics, computer science and technology*, Springer, pp 453–460

Jajodia, S., Liu, P., Swarup, V., Wang, C., 2009. *Cyber Situational Awareness*. Springer.

Kaber, D.B., Endsley, M.R., 1998. Team situation awareness for process control safety and performance. *Process Saf. Prog.* 17 (1), 43–48.

- Kabir, M.E., Wang, H., Bertino, E., 2012. A role-involved purpose-based access control model. *Information Systems Frontiers* 14 (3), 809–822.
- Kane, G. C., Phillips, A. N., Copulsky, J. R., & Andrus, G. R. (2019). *The technology fallacy: How humans are the real key to digital transformation*. Cambridge, Massachusetts: The MIT Press.
- Khallaf, A., & Majdalawieh, M. (2012). Investigating the Impact of CIO Competencies on IT Security Performance of the U.S. Federal Government Agencies. *Information Systems Management*, 29(1), 55-78. <https://doi.org/10.1080/10580530.2012.634298>
- Khan, S., and Madnick, S. 2019. "Cybersafety: A System-Theoretic Approach to Identify Cyber-Vulnerabilities & Mitigations in Industrial Control Systems," Available at SSRN 3542551).
- Kline, R. B. (2005) *Principles and Practice of Structural Equation Modeling*, New York, London, The Guilford Press.
- Knapp ED, Langill JT (2014) *Industrial network security: securing critical infrastructure networks for smart grid, SCADA, and other industrial control systems*. Syngress, Burlington
- Kordy, B., Wide, W., 2018. On quantitative analysis of attack defense trees with repeated labels. In: *International Conference on Principles of Security and Trust*. Springer, pp. 325–346.
- Kriaa S, Pietre-Cambacedes L, Bouissou M, Halgand Y (2015) A survey of approaches combining safety and security for industrial control systems. *Reliab Eng Syst Saf* 139:156–178
- Krumay B, Bernroider EWN, Walser R (2018) Evaluation of cyber security management controls and metrics of critical infras-tructures: a literature review considering the NIST CybersecurityFramework. In: Gruschka N. (ed) *NordSec. Lecture Notes in Com-puter Science*, vol 11252, pp 369–384.
- Lambrinouidakis, C.; Gritzalis, S.; Xenakis, C.; Katsikas, S.; Karyda, M.; Tsochou, A.; Papadatos, K.; Rantos, K.; Pavlosoglou, Y.; Gasparinatos, S.; et al. *Compendium of Risk Management Frameworks with Potential Interoperability: Supplement to the Interoperable EU Risk Management Framework Report*; European Union Agency for Cybersecurity (ENISA): Athens, Greece, 2022; ISBN 9789292045548.
- Lidster, William & Rahman, Shawon. (2018). *Obstacles to Implementation of Information Security Governance*. 1826-1831. 10.1109/TrustCom/BigDataSE.2018.00276.

- Lopes, I.M.; Guarda, T.; Oliveira, P. Implementation of ISO 27001 Standards as GDPR Compliance Facilitator. *J. Inf. Syst. Eng. Manag.* **2019**, *4*, em0089.
- M. Endsley. Toward a theory of situation awareness in dynamic systems. In *Human factors Journal*, volume 37(1), pages 32–64, March 1995
- Macpherson, W. G., Lockhart, J. C., Kavan, H., & Iaquinto, A. L. (2015). Kaizen: A Japanese philosophy and system for business excellence. *Journal of Business Strategy*, *36*(5), 3-9.
<https://doi.org/10.1108/JBS-07-2014-0083>
- Madsen, W. (2013). Reinventing Federal Security Policy: A Failed Effort. *Information Systems Security*, *4*(1), 11-15. <https://doi.org/10.1080/10658989509342484>
- Maedche, A. (2016). Interview with Michael Nilles on “What Makes Leaders Successful in the Age of the Digital Transformation?”. *Business & Information Systems Engineering*, *58*(4), 287-289.
[doi:10.1007/s12599-016-0437-1](https://doi.org/10.1007/s12599-016-0437-1)
- Maheshwari, R., & Pathak, S. (2012). A Proposed Secure Framework for Safe Data Transmission, in Private Cloud. *International Journal of Recent Technology and Engineering*, *1*(1), 78–8
- Malatji, M. Management of enterprise cyber security: A review of ISO/IEC 27001:2022. In *Proceedings of the 2023 International Conference on Cyber Management and Engineering, CyMaEn 2023*, Bangkok, Thailand, 26–27 January 2023. [Google Scholar]
- Masaaki, I. (1986). *Kaizen: The key to Japan's competitive success*. New York, Ltd: McGraw-Hill.
- Matt, C., Hess, T., & Benlian, A. (2015). Digital transformation strategies. *Business & Information Systems Engineering*, *57*(5), 339-343.
- Meraviglia, L. (2018). Technology and counterfeiting in the fashion industry: Friends or foes? *Business Horizons*, *61*(3), 467-475.
- Meyer, T., & Reniers, G. (2013). *Engineering risk management*. Berlin: De Gruyter Graduate.
- Mujinga, Mathias & Eloff, Mm & Kroeze, Jan. (2017). A socio-technical approach to information security.
- Mumford, E. (2006), “The story of socio-technical design: reflections on its successes, failures and potential”, *Information Systems Journal*, Vol. 16 No. 4, pp. 317-342

- National Institute of Standards and Technology (NIST): NIST SP 800-53 Rev. 4 Recommended Security Controls for Federal Information Systems and Organizations U.S. Government Printing Office (2013). URL:
http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final{_}updated-errata{_}05-01-2010.pdf
- Nazir, H.M.J., Han, W., 2022. Proliferation of cyber situational awareness: today's truly pervasive drive of cybersecurity. In: Security and Communication Networks, p. 2022
- Newitt, D. (1996). Beyond BPR & TQM-Managing through processes: Is Kaizen enough? Paper presented NIST: FIPS PUB 199: Standards for Security Categorization of Federal Information and
- NIST. NIST special publication 800-82 guide to industrial control systems (ICS) security. 2011
- Noel, S., 2018. A Review of Graph Approaches to Network Security Analytics. Springer International Publishing, Cham, pp. 300–323, https://doi.org/10.1007/978-3-030-04834-1_16.
- Page, C. & Meyer, D. (2000) Applied Research Design for Business and Management, Sydney, McGraw-Hill Companies, Inc.
- Pahi, T., Leitner, M., Skopik, F., 2017. Analysis and assessment of situational awareness models for national cyber security centers. In: ICISSP 2017 - Proceedings of the 3rd International Conference on Information Systems Security and Privacy, pp. 334–345.
- Paja, Elda & Dalpiaz, Fabiano & Giorgini, Paolo. (2015). Modelling and Reasoning about Security Requirements in Socio-Technical Systems. Data & Knowledge Engineering. 98. 10.1016/j.datak.2015.07.007.
- Parker, D. B. (1995). 'A New Framework for Information Security to Avoid Information Anarchy', Information Security — the Next Decade: Proceedings of the IFIP TC11 eleventh international conference on information security, IFIP/Sec '9, https://doi.org/10.1007/978-0-387-34873-5_13
- Paté-Cornell, M.E., Kuypers, M., Smith, M., Keller, P., 2018. Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies. Risk Analysis 38 (2), 226–241.
- Perkin, N., & Abraham, P., (2017). Building the Agile Business through Digital Transformation. Kogan Page Publishers.

- Poljanšek, K. et al. Recommendations for National Risk Assessment for Disaster Risk Management in EU. (Publications Office of the European Union, 2019). doi:10.2760/084707 (online)
- Posthumus S, Von Solms R. A framework for the governance of information security. *Comput. Secur.* 2004a;23(8):638–46. doi:10.1016/j.cose.2004.10.006
- Purdy, G. ISO 31000:2009—Setting a new standard for risk management. *Risk Anal.* 2010, 30, 881–886.
- Purdy, G. ISO 31000:2009—Setting a new standard for risk management. *Risk Anal.* 2010, 30, 881–886.
- Ramani, G. & Kumar, V. (2008) 'Interaction Orientation and Firm Performance'. *Journal of Marketing*, Vol.72 No.1, pp.27-45.
- Renn, O. (2008). *Risk governance: Coping with uncertainty in a complex world*. London: Earthscan.
- Rogers, D. L., (2016). *The Digital Transformation Playbook : Rethink Your Business for the Digital Age*. New York: Columbia Business School Publishing.
- Rokkan, A. I., Heide, J. B. & Wathne, K. (2003) 'Specific Investments in Marketing Relationships'. *Journal of Marketing Research*, Vol.40 No.2, pp.210-224.
- Rouhani, S.; Belchior, R.; Cruz, R.S.; Deters, R. Distributed attribute-based access control system using permissioned blockchain. *World Wide Web* 2021, 24, 1617–1644.
- S. Kabanda, M. Tanner, and C. Kent, "Exploring SME cybersecurity practices in developing countries," *J. Organ. Comput. Electron. Commer.*, vol. 28, no. 3, pp. 269–282, 2018.
- S. Kabanda, M. Tanner, and C. Kent, "Exploring SME cybersecurity practices in developing countries," *J. Organ. Comput. Electron. Commer.*, vol. 28, no. 3, pp. 269–282, 2018.
- Saini, Vineet & Duan, Qiang & Paruchuri, Vamsi. (2008). Threat Modeling Using Attack Trees. *Journal of Computing Sciences in Colleges*. 23.
- Salmon, P.M., Stanton, N.A., Walker, G.H., Baber, C., Jenkins, D.P., McMaster, R., et al., 2008. What really is going on? Review of situation awareness models for individuals and teams. *Theor. Issues Ergon. Sci.* 9 (4), 297–323.
- Salmon, P.M., Stanton, N.A., Walker, G.H., Jenkins, D., Ladva, D., Rafferty, L., et al., 2009. Measuring Situation Awareness in complex systems: comparison of measures study. *Int. J. Ind. Ergon.* 39 (3), 490–500.

- Salmon, P.M., Stanton, N.A., Walker, G.H., Jenkins, D.P., 2017. Distributed Situation awareness: Theory, Measurement and Application to Teamwork. CRC Press.
- Sandberg H, Amin S, Johansson K (2015) Cyberphysical security in networked control systems: an introduction to the issue. *IEEE Control Syst* 35:20–23
- Sasse, M. A., Brostoff, S., and Weirich, D. 2001. "Transforming the 'Weakest Link'—a Human Computer Interaction Approach to Usable and Effective Security," *BT Technology Journal* (19:3), pp. 122-131.
- Schinagl, S., & Shahim, A. (2020). What do we know about information security governance? "From the basement to the boardroom": towards digital security governance. 10.1108/ics-02-2019-0033
- Schneier, Bruce, Attack Trees, *Dr. Dobb's Journal of Software Tools* 24, 12(December 1999): 21-29.
- Seongmo. An & Eom, Taehoon & Park, Jong & Hong, Jin & Nhlabatsi, Armstrong & Fetais, Noora & Khan, Khaled & Kim, Dan. (2019). CloudSafe: A Tool for an Automated Security Analysis for Cloud Computing. 602-609. 10.1109/TrustCom/BigDataSE.2019.00086.
- Silva Rampini, G.H.; Takia, H.; Tobal Berssaneti, F. Critical Success Factors of Risk Management with the Advent of ISO 31000 2018—Descriptive and Content Analyzes. *Procedia Manuf.* **2019**, 39, 894–903. [Google Scholar] [CrossRef]
- Sofi, A. Bluetooth Protocol in Internet of Things (IoT), Security Challenges and a Comparison with Wi-Fi Protocol: A Review. *Int. J. Eng. Tech. Res.* 2016, 5, 1–7.
- Souppaya, M., Scarfone, K.: NIST Special Publication 800-124 Rev. 1 Guidelines for Managing the Security of Mobile Devices in the Enterprise. NIST special publication p. 30 (2013). DOI 10.6028/NIST.SP.800-124r1
- Steenkamp, J. B. E. M. & van Trijp, H. C. M. (1991) 'The Use of LISREL in Validating Marketing Constructs'. *International Journal of Research in Marketing*, Vol.8 No.4, pp.283-299.
- Steinbart, P.J., Keith, M.J., Babb, J., 2016. Examining the continuance of secure behavior: A longitudinal field study of mobile device authentication. *Information Systems Research* 27 (2), 219–239.
- Stewart, H., and Jürjens, J. (2017), "Information security management and the human aspect in organizations", *Information & Computer Security*, vol. 25, no. 5, pp. 494–534. <https://doi.org/10.1108/ICS-07-2016-0054>.

- Stewart, H., and Jürjens, J. (2018), "Data security and consumer trust in FinTech innovation in Germany", *Information & Computer Security*, vol. 26, no. 1, pp. 109–128.
<https://doi.org/10.1108/ICS-06-2017-0039>.
- Stewart, H. (2021), "The hindrance of cloud computing acceptance within the financial sectors in Germany", *Information and Computer Security*, Vol. ahead-of-print No. ahead-of-print.
<https://doi.org/10.1108/ICS-01-2021-0002>
- Stewart, H. (2022), "A systematic framework to explore the determinants of information security policy development and outcomes", *Information and Computer Security*, Vol. 30 No. 4, pp. 490-516.
<https://doi.org/10.1108/ICS-06-2021-0076>
- Stewart, H. (2022) 'Digital Transformation Security Challenges, *Journal of Computer Information Systems*, DOI: 10.1080/08874417.2022.2115953
- Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., Hahn, A.: NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security Revision 2. Tech. rep., NIST (2015)
- Suárez-Barraza, M. F., & Lingham, T. (2008). Kaizen within Kaizen teams: continuous and process improvements in a Spanish municipality. *Asian Journal on Quality*, 9(1), 1-21.
- Sulistiyowati, D.; Handayani, F.; Suryanto, Y. Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss. *Int. J. Inform. Vis.* **2020**, 4, 225–230. [Google Scholar] [CrossRef]
- Sveen, F. O., Torres, J. M., and Sarriegi, J. M. 2009. "Blind Information Security Strategy," *International Journal of Critical Infrastructure Protection* (2:3), pp. 95-109.
- Tang, J., Wang, D., Ming, L., & Li, X. (2012). A Scalable Architecture for Classifying Network Security Threats. *Science and Technology on Information System Security Laboratory*.
- Tarazan, S, and Bostan, A. 2016. "Customizing SSL Certificate Extensions to Reduce False-Positive Certificate Error/Warning Messages," *International Journal of Information Security Science* (5:2), pp. 21-28.
- Tatiara, R.; Fajar, A.N.; Siregar, B.; Gunawan, W. Analysis of factors that inhibiting implementation of Information Security Management System (ISMS) based on ISO 27001. In *Proceedings of the Journal of Physics: Conference Series, Medan, Indonesia, 28–30 November 2018; Volume 978*.

- Teece, D.J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal*, 28, 1319–1350.
- Teece, D.J. (2018). Dynamic capabilities as (workable) management systems theory. *Journal of Management and Organization*, 24, 359–368.
- Toapanta, M., Nazareno, J., & Tingo, R. (2016). Analysis of the Appropriate Security Models to Apply in a Distributed Architecture. IOP Conference Series: Materials Science and Engineering. Guayaquil, Ecuador: IEEE.
- Troyer, L. (2017), “Expanding sociotechnical systems theory through the trans-disciplinary lens of complexity theory”, in Kahlen, J., Flumerfelt, S. and Alves, A. (Eds.), *Transdisciplinary Perspectives on Complex Systems*, Springer, Cham.
- Ulven, J.B., and G. Wangen. 2021. A systematic review of cybersecurity risks in higher education. *Future Internet* 13 (2): 1–40. <https://doi.org/10.3390/fi13020039>.
- Urbach, N., & Röglinger, M. (2018). Introduction to Digitalization Cases. How Organizations Rethink Their Business for the Digital Age. In N. Urbach & M. Röglinger (2018), *Digitalization Cases. How Organizations Rethink Their Business for the Digital Age*. (pp. 1-14). Cham, Switzerland: Springer.
- Vejvodová, P. (2019). Information and Psychological Operations as a Challenge to Security and Defence. *Vojenské Rozhledy*, 28(4), 83-96. <https://doi.org/10.3849/2336-2995.28.2019.03.083-096>
- Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, 28(2), 118-144.
- von Leipzig, T., Gamp, M., Manz, D., Schöttle, K., Ohlhausen, P., Oosthuizen, G., Palm, D., & von Leipzig, K., (2017). Initialising Customer-Orientated Digital Transformation in Enterprises. *Procedia Manufacturing* (8), 517-524.
- Von Solms B. Corporate governance and information security. *Comput. Secur.* 2001;20(3):215–18.
- W. E. Deming: *Out of the Crisis*. Massachusetts Institute of Technology, Cambridge 1982, ISBN 0-911379-01-0, S. 88.
- Warner, K.S.R., & Wäger, M. (2019). Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal. *Long Range Planning*, 52, 326–349

- Wessel, L., Baiyere, A., Ologeanu-Taddei, R., Cha, J., & Jensen, T. B., (2020). Unpacking the Difference between Digital Transformation and IT-Enabled Organizational Transformation. *Journal of Association of Information Systems*, 22(1), 102-129
- Whitman, Michael & Mattord, Herb. (2014). Information Security Governance for the Non-security Business Executive. 11. 97-111
- Y. Barlette, K. Gundolf, and A. Jaouen, "CEOs' information security behavior in SMEs: Does ownership matter?" *Syst. d'information Manag.*, vol. 22, no. 3, pp. 7–45, 2017.
- Y. Barlette, K. Gundolf, and A. Jaouen, "CEOs' information security behavior in SMEs: Does ownership matter?" *Syst. d'information Manag.*, vol. 22, no. 3, pp. 7–45, 2017.
- Yahoo (2023) Data Leakage*. Available from: shorturl.at/EMRY7 [accessed Jan 05 2023]. Yang, M.-X.
- Yuan, L.-N., & Yang, Z.-X. (2010). A discuss of computer security strategy models. *International Conference on Machine Learning and Cybernetics* (pp. 20-33). Qingdao, China: IEEE.
- Yee, K. P. 2004. "Aligning Security and Usability," *IEEE Security & Privacy* (1:5), pp. 48-55.
- Yu, H.J.; Kim, C.H.; Im, S.S.; Oh, S.H. ZigBee Authentication Protocol with Enhanced User Convenience and Safety. *J. Inf. Secur.* 2022, 22, 81–92.
- Adeyoku, A. (2019). Cybercrime and Cybersecurity: FinTech's Greatest Challenges. Available at SSRN 3486277.
- Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69, 437-443.
- B. Moule and L. Giavara, —Policies, procedures and standards: an approach for implementation, *Inf. Manag. Comput. Secur.*, vol. 3, no.3, pp. 7–16, 1995.
- Barbu CM, Florea DL, Dabija D-C, Barbu MCR. Customer experience in fintech. *J Theor Appl Electron Commerce Res.* 2021;16(5):1415–33. doi:10. 3390/jtaer16050080.
- Bassett G, Hylender CD, Langlois P, Pinto A, Widup S. Data breach investigations report. Verizon DBIR Team, Tech Rep; 2021

- Carlton, M. (2016). Development of a cybersecurity skills index: A scenarios-based, hands-on measure of non-IT professionals' cybersecurity skills. Doctoral dissertation. Nova Southeastern University.
- Casoria M. Cybersecurity as enterprise risk within and beyond the Bahraini legal framework. *KnE Eng.* 2018;3:37–51. doi:10.18502/keg.v3i7.3071.
- D. F. Sterne, —On the Buzzword?? Security Policy??" 1991, p. 219.
- D. W. Arnesen and W. L. Weis, —Developing an effective company policy for employee internet and email use,|| *J. Organ. Cult. Commun.Confl.*, vol. 11, no. 2, p. 53, 2007.
- D'Arcy, J., & Devaraj, S. (2012). Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decision Sciences*, 43(6), 1091e1124.
- D'Arcy, J., Gupta, A., Tarafdar, M., & Turel, O. (2014). Reflecting on the “dark side” of information technology use. *Communications of the Association for Information Systems*, 35(5), 109e118.
- D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security counter-measures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1), 79e98.
- Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017). Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace. *Computers in Human Behavior*, 67, 196e206.
- Davis K, Maddock R, Foo M. Catching up with Indonesia’s fintech industry. *Law Financ Mark Rev.* 2017;11(1):33–40. doi:10.1080/17521440.2017.1336398.
- Doherty, N.F., and H. Fulford H. (2006) "Aligning The Information Security Policy with The Strategic Information Systems Plan." *Comput Secur* 25 : 55–63. doi:10.1016/j.cose.2005.09.009.
- Elhai, J. D., Chai, S., Amialchuk, A., & Hall, B. J. (2017). Cross-cultural and gender associations with anxiety about electronic data hacking. *Computers in Human Behavior*, 70, 161-167.
- Eyal I. Blockchain technology: transforming libertarian cryptocurrency dreams to finance and banking realities. *Computer.* 2017;50(9):38–49. doi:10.1109/MC.2017. 3571042.

- Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding non-malicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, 28(2), 203e236.
- H.S. Lallie, L.A. Shepherd, J.R. Nurse, A. Erola, G. Epiphaniou, C. Maple, X. Bellekens Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic *Comp. Security*, 105 (2021), Article 102248
- Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, 43(4), 615-660.
- J. Rees, S. Bandyopadhyay, and E. H. Spafford, —PFIRES: A Policy Framework for Information Security, *Commun. ACM*, vol. 46, no. 7, pp. 101–106, Jul. 2003.
- K. A. Loggie et al., —An analysis of copyright policies for distance learning materials at major research universities, *J. Interact. Online Learn.*, vol. 5, no. 3, pp. 224–242, 2006.
- K. R. Lindup, —A new model for information security policies, *Comput. Secur.*, vol. 14, no. 8, pp. 691–695, 1995
- Kaufman, L.M., Data security in the world of cloud computing. *Security & Privacy, IEEE*, 7(4) (2009) 61-64.
- Kaur G, Habibi Lashkari Z, Habibi Lashkari A, Kaur G, Habibi Lashkari Z, Habibi Lashkari A. Chapter 8- Cybersecurity policy and strategy management in FinTech. *Understanding Cybersec Manage FinTech*. 2021;153–66.
- M. T. Siponen, —Policies for construction of information systems' security guidelines, *in IFIP International Information Security Conference*, 2000, pp. 111–120.
- M. Winniford, S. Conger and L. Erickson-Harris, "Confusion in the Ranks," *Information Systems Management*, Vol. 26, No. 2, 2009, pp. 153-163.
- Mehrban S, Nadeem MW, Hussain M, Ahmed MM, Hakeem O, Saqib S, Kiah, M.M., Abbas, F., Hassan, M., Khan, M.A. Towards secure FinTech: a survey, taxon-omy, and open research challenges. *IEEE Access*. 2020;8:23391–406. doi:10.1109/ACCESS.2020.2970430

- Mladenow, A., et al. Value Creation Using Clouds: Analysis of Value Drivers for Start-Ups and Small and Medium Sized Enterprises in the Textile Industry. in *Advanced Information Networking and Applications Workshops (WAINA)*, 2012 26th International Conference on. (2012). IEEE.
- Modi, C., et al., A survey on security issues and solutions at different layers of Cloud computing. *The Journal of Supercomputing*. 63(2) (2013) 561-592.
- N. F. Doherty, L. Anastasakis, and H. Fulford, —The information security policy unpacked: A critical study of the content of university policies, *Int. J. Inf. Manage.*, vol. 29, no. 6, pp. 449–457, 2009
- Najaf K, Schinckus C, Yoong LC. VaR and market value of fintech companies: an analysis and evidence from global data. *Manage Financ*. 2020;47(7):915–36. doi:10.1108/MF-04-2020-0169.
- Newhouse, B. K., Scribner, B., & Witte, G. (2016). NICE cybersecurity workforce framework (NCWF). Draft NIST special publication 800, 181. Retrieved at <https://doi.org/10.6028/NIST.SP.800-181>.
- R. Baskerville and M. Siponen, —An information security meta-policy for emergent organizations, *Logist. Inf. Manag.*, vol. 15, no. 5/6, pp. 337–346, 2002
- Schneier, B. (2011). *Secrets and lies: Digital security in a networked world*. Hoboken, NJ: John Wiley & Sons.
- Schueffel P. Taming the beast: a scientific definition of fintech. *J Innovation Manage*. 2016;4(4):32–54. doi:10.24840/2183-0606_004.004_0004.
- Shillair, R., Cotten, S. R., Tsai, H. Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, 48, 199e207.
- Stewart, H., and Jürjens, J. (2017), "Information security management and the human aspect in organizations", *Information & Computer Security*, vol. 25, no. 5, pp. 494–534. <https://doi.org/10.1108/ICS-07-2016-0054>.
- Stewart, H. (2021), "The hindrance of cloud computing acceptance within the financial sectors in Germany", *Information and Computer Security*, Vol. ahead-of-print No. ahead-of-print. <https://doi.org/10.1108/ICS-01-2021-0002>

- Stewart, H. (2022), "A systematic framework to explore the determinants of information security policy development and outcomes", *Information and Computer Security*, Vol. 30 No. 4, pp. 490-516.
<https://doi.org/10.1108/ICS-06-2021-0076>
- Taylor PJ, Dargahi T, Dehghantanha A, Parizi RM, Choo K-K. A systematic literature review of blockchain cyber security. *Digital Comm Netw.* 2020;6(2):147–56. doi:10.1016/j.dcan.2019.01.005.
- Vučinić M, Luburić R. Fintech, risk-based thinking and cyber risk. *J Cent Banking Theory Pract.* 2022;11(2):27–53. doi:10.2478/jcbtp-2022-0012
- W. Auyporn, K. Piromsopa, T. Chaiyawat Critical Factors in Cybersecurity for SMEs in Technological Innovation Era ISPIM Conference Proceedings, The International Society for Professional Innovation Management (ISPIM) (2020), pp. 1-10
- Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6), 2799e2816.
- Y. Barlette and V. Fomin, "Exploring the suitability of IS Security Management Standards for SMEs," In: R. H. Sprague, Ed., *Proceeding of 41st Hawaii International Conference on System Sciences (HICSS)*, Los Alamitos, 2008, pp. 308- 317.

Chapter 3. Methodology

3.1. Overview

This study develops a new holistic cybersecurity model called the Nine Five Circle (NFC), distinguishing itself from mainstream contemporary information security literature. This pioneering NFC model provided by this research has already been peer-reviewed, published, and applied in a real-life industry scenario in practice.

This chapter is organised into two parts. The first section justifies the research design comprising exploratory, descriptive, and causal research. In this study, both qualitative and quantitative methods are used as part of a multi-method approach. Qualitative research is beneficial in the exploratory research phase for forming a conceptual model and generating a hypothesis (Ticehurst & Veal, 2000; Davidson, 2009; Marcuschi, 2007). It forms the basis for quantitative research in this thesis and uniquely combines IS and DT security. In this thesis, the quantitative research should help extend the theory of IS security and DT security and provide explanatory or causal evidence.

3.2. Research Design

This research approach uses data analysis to connect collected data with research questions. It is based on the work of Cooper and Schindler (2006), Ghauri and Gronhaug (2005), and Yin (2014) and combines exploratory, descriptive, and causal research.

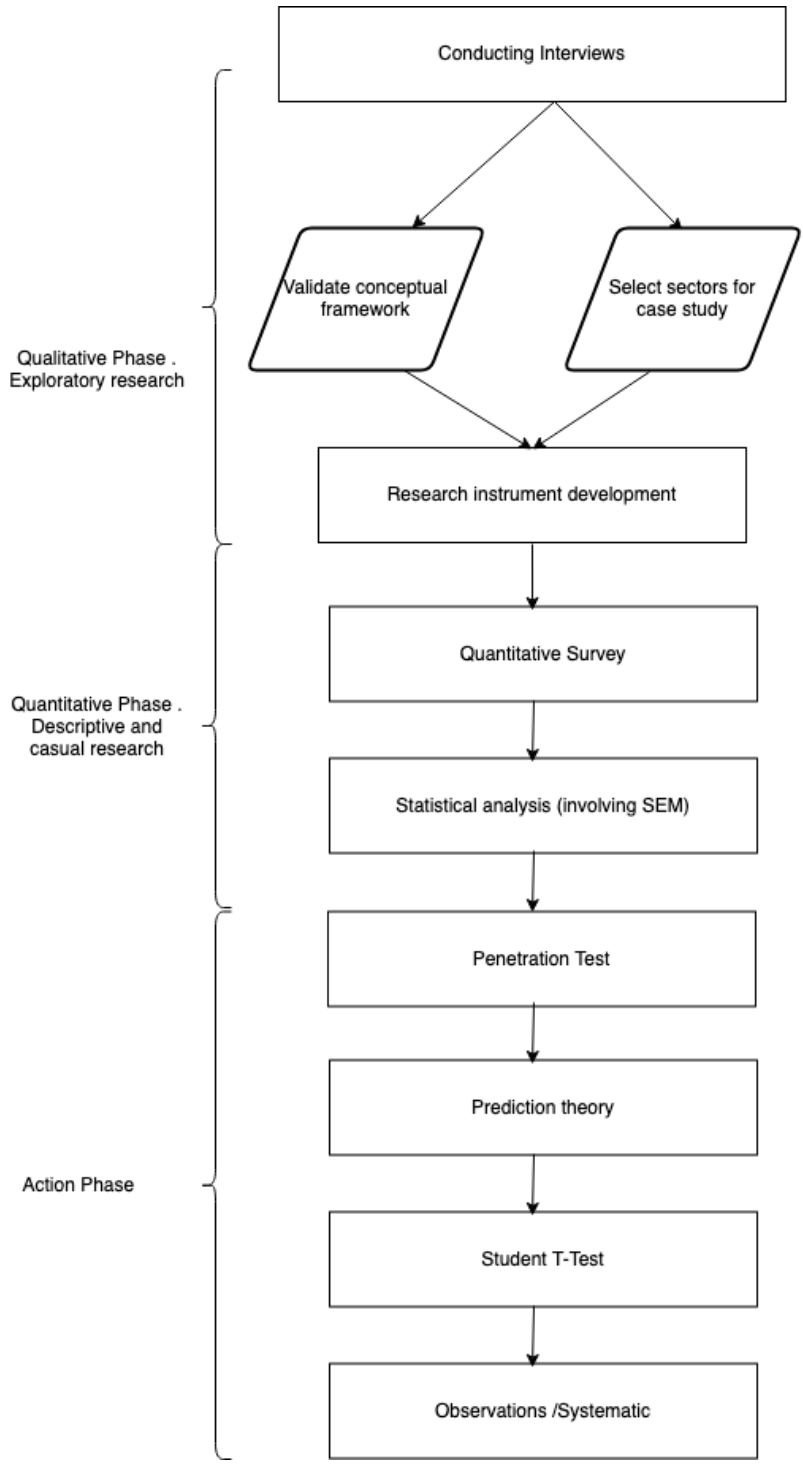


Fig. 5. Flowchart depicting the research design

Figure 5 above depicts the two main qualitative and quantitative research areas that form the basis of this research, starting with exploratory research, followed by descriptive and causal research. This research methodology integrated a multiple-case design that supports empirical research by providing units of measurement (Yin, 2014).

The study relies on input from innovative industries and consumers (Farías & Montero, 2005). It includes multiple case studies across various sectors. Yin (2014) identifies three case study approaches: descriptive, exploratory, and explanatory. These approaches can produce qualitative and quantitative findings (Eisenhardt, 1989) and are all used in this research to develop a new theory with innovative outcomes.

A. Qualitative Phase (Exploratory Research)

Due to the novelty of this research, the qualitative research methods are used in the exploratory phase and contribute to the development of the conceptual framework and help to justify the NFC model proposed. Given the combination of two domains: IS and DT, in this work in a novel method, it is helpful to explore with key informants to pinpoint significant variables and correlations assigned to their respective constructs. Explanatory variables that cannot be measured are called constructs (Farías & Montero, 2005). As a result, it is critical to develop hypotheses and ensure that the research is valuable and relevant to practitioners.

It also helps to determine the feasibility of a formal survey to identify early participants in the selected industries, such as conducting key informant interviews. It assists in refining the conceptual framework and facilitates the development of research instruments for other empirical studies (Blaxter et al., 2001). Studies on improving security in DT strategy and IS are based on a few empirical studies. A limited number of studies focus on the units of analysis, usually on a particular organisation or focus group (Provan & Milward, 1995). Similarly, the operational definitions and variables used today are specific to a particular organisation or group. Thus, exploratory research is necessary to develop a research instrument, operational definitions, and variables that reflect a holistic level of in-depth analysis.

B. Quantitative Phase (Descriptive & Casual Research)

A quantitative study was performed following the qualitative research, which revealed that previous studies emphasise the benefits of DT without conducting an empirical analysis of the security

challenges that hinder this transition (Stewart, 2022) and, in other instances, limit themselves to a privacy standpoint.

To improve the ability to test theories and gain a better understanding of the intersection of information security and digital technology, empirical research is essential. Given the lack of quantitative research on this topic and the urgent demand for a secure DT, descriptive and explanatory studies are relevant.

To fully understand cybersecurity in the context of IS and DT, it is essential to conduct descriptive research. This type of research involves analysing variables to determine their characteristics, proportions, and relationships through means and variances (Cooper and Schindler, 2006). Given that research in IS and DT mainly involves ideas and concepts, creating structure and formality is crucial. Descriptive research is a transitional phase and sets the foundation for future explanatory research.

Furthermore, this approach was chosen because of the quantitative survey, which indirectly quantifies the obstacles to DT. It is assumed that the causes of sluggish demand lie in various challenges. The indirect measurement is done by combining numerous variables that result in a variable that will be discussed later. In a conceptual map, variables are the observable and quantifiable characteristics that are closely related to observable facts. Furthermore, variables can be divided into dependent variables, which are influenced by the independent variable, and independent variables, each with measurable characteristics.

Consequently, the independent variable leads to the dependent variable (Hair, et al., 2007, p. 144). As indicated earlier, these variables are organised into constructs to describe and predict various characteristics. Revisions can be made to improve the constructs. As a result, a construct is an explanatory variable or a collection of characteristics that contribute to understanding the construct.

The positivist research technique is commonly applied in information systems (Easterby-Smith et al., 2002). Positivism, a scientific-theoretical view, assumes that knowledge is based on positive facts, not emotions. Positivism rejects everything scientific experiments, or ethical and theological analyses cannot prove. The observable part of society explored during the research process can be used to draw a generalisation about the whole society. The methodology of data collection for this research is based on existing theory. This was addressed in the previous literature review to develop the research hypothesis to be proven or disproven. If the hypotheses are proven wrong, further theories need to be explored. The positivist method also assumes constant scientific progress and objectivity on the

researcher's part. It is not easy to remain unbiased during the research process, as the researcher may feel personal opinions or empathy toward the study participants.

This research topic goes beyond mere description and aims to identify patterns and trends through explanatory or causal research (Ticehurst and Veal, 2000). The focus is on addressing the security challenges that hinder the success of DT and IS strategy. Establishing causality can improve the theory's predictive potential and offer practical management implications for policymakers and innovators. To test the hypotheses of the research, the partial least squares structural equation modelling (PLS-SEM) method is used instead of covariance-based structural equation modelling (CB-SEM) as it provides more reliable results for small sample sizes and non-multivariate normality data. The conceptual framework is assessed for significance and relevance using the coefficient of determination (R^2) and effect size (f^2) (Hair et al., 2011). This study uses a cross-sectional approach to determine both the causes and effects.

3.3. Qualitative Research Methods Step

3.3.1. Overview

The data collection process was in two stages, as in the work of Walsham's study (2006), which involved (1) case studies and interviews, and (2) participant observation (Creswell, 2010). The data collection phase consisted of an anonymous open-ended survey, in-depth interviews, and case study analysis (Goudy & Potter, 1975; Lavin & Maynard, 2001).

3.3.2. Case Studies

The qualitative case study design incorporates ethnographic data collection and analysis, selecting three sectors as sampling units based on size and participation in DT (Creswell, 1998; Denzin & Lincoln, 2000; Yin, 2014). Ethnography involves multiple strands, allowing for triangulation across various data sources. Once the innovative sectors are identified, they are considered the unit of measurement, and respondents' organisations serve as sampling units for the subsequent quantitative study. Case studies can be combined with qualitative and quantitative research as a complementary and coordinated strategy (Yin, 2014). Embedded case studies are preferred over holistic case studies, as they identify sample sub-units, resulting in high-quality case studies (Yin, 2014). All employees were initially interviewed in realistic social situations and forms to combat the focus groups' divergent nature (Morgan & Krueger, 1998). The interconnectedness of the sectors in this research enabled the use of a unique case study technique (Iacobucci, 1996). This research applies the case study to explore security challenges and find solutions to underlying transformation processes. The pilot study focuses on a

single industry and its clients. In contrast, the comprehensive field research focuses on three different sectors intentionally chosen to contradict each other, enabling the identification of patterns and trends. Other industries can apply the results.

3.3.3. Interviews

This study employs a semi-structured methodology in which the questions for consumers and organisations are different but are asked in the same order throughout all interviews. It helps in exploring the subject's opinions, behaviour, experiences, and perception of the subject (Cooper & Schindler, 2006). The duration of each interview is 45 minutes. Conducting these interviews is necessary, given the innovative nature of the field of study.

The interview questions were open-ended (Britten, 1995) so that in-depth information can be gathered (Kumar, 1996). The interview began with simple questions that participants could easily respond to before moving on to more complex and sensitive topics. This approach creates a comfortable environment for the interviewee, fosters rapport (Goudy & Potter, 1975; Lavin & Maynard, 2001) and trust, and provides rich data that can be used to further refine the interview (Stewart & Jürjens 2018; Britten, 1999).

It was necessary to choose the semi-structured approach over the structured and unstructured strategy because of the nature of this research and the requirement to review new factors explored in the literature. Semi-structured questions are loosely structured and provide more opportunities for respondents to fully express themselves, enable analysis, and contribute to developing the conceptual framework derived from the literature. They are more likely to contribute to theory development than the unstructured and structured techniques (Adams, 2005).

There were three distinct interview stages: The first round of interviews aimed to select consumers of digital products to analyse their perceptions of digital products and services for further analysis and development of a conceptual model. The second set of interviews targeted the financial sector to analyse their perception of the shift to the cloud for further analysis and development of a conceptual model. The third set of interviews aimed to select two more organisations, including the financial sector, to analyse their security challenges related to DT and security for further analysis and development of a conceptual model and the NFC model to address these challenges and propose workarounds to strengthen cybersecurity in DT. In the first and second interviews, respondents were first asked to give examples of digital products and services they know. Then they were asked to name the key factors that hinder them from adopting these disruptive innovations. In the third interview,

respondents were first asked to give examples of security challenges they were aware of in their organisation. The significant factors that the respondents considered critical for the achievement of DT were then examined, as well as their perspectives on the role of security in this innovation. The interviewees were given a presentation on the conceptual framework that resulted from the literature research at the end of the interview. It was discussed whether the elements found in the framework were relevant.

The key informants from the consumer sector and those from the three sectors of finance, automotive and fintech were selected using a dimensional quota method and presented in Tables 3 and 4, respectively (Abi et al., 2017). Dimensional sampling is a sampling technique that extends quota sampling. The researcher selects multiple characteristics such as gender, age, income, residence, and education and ensures that at least one participant is included for each chosen characteristic (Arnold, 1970). In this method, informants are selected within each key dimension of the population under study to ensure that each dimension is represented in the sample (Sarantakos, 1998). Pre-selection calls, social media platforms, online and live panel providers, dedicated panels, face-to-face interviews, website reviews, key government agencies, trade associations, industry studies and annual reports were used to select representatives for each dimension. Interviews with key informants and security experts in each industry were deemed necessary to understand the networks and determine the applicability and relevance of this research. Interviewees were selected using a systematic sampling method (see Table 3).

Systematic sampling based on picking every n th person where:

$$n = \text{sample population} / \text{sample size} \quad (1)$$

Table 3. Demographic of digital products users' participants

Variables		TOTAL
Gender		
	Male	60%
	Female	40%
Age		
	18-30 years	20%
	31-40 years	35%
	41-50 years	40%
	50 + years	5%

Position		
	Senior Directors	15%
	Functional Directors	20%
	IT Specialists	15%
	Personnel	20%
	Others	30%
Participants from each CASE		
	CASE 1 – Banks	60%
	CASE 2 – Automobiles	25%
	CASE 3 - FINTECH Start-ups	10%

Table. 4. Industrial participants and key informants

Industry		Position	Interviewee (Anonymous ID)
Finance	Banks	Senior executives, CIO	IDR_##
		Digital Strategy Manager	IDR_##
		IT Decision Maker	IDR_##
		IT-Staff & Network	IDR_##
		DevOPs	IDR_##
		Staff	IDR_##
Start-ups	FinTech	Senior executives, CIO	IDR_##
		Digital Strategy Manager	IDR_##
		IT Decision Maker	IDR_##
		IT-Staff & Network	IDR_##
		Staff	IDR_##
Automobile	Car industries	DevOPs	IDR_##
		Digital Strategy Manager	IDR_##
		IT Decision Maker	IDR_##
		IT-Staff & Network	IDR_##
		DevOPs	IDR_##
		Staff	IDR_##

The second round of interviews thoroughly examined the results from the first and second rounds. These interviews were conducted to identify and address security challenges related to DT and to determine the organisations that would be selected for further study. The fintech organisation was chosen for a pilot study, while the other two organisations were selected for in-depth field research. These sectors were selected because they are undergoing rapid changes and can be quantitatively evaluated.

The interviews were necessary because there is limited empirical research on DT and IS (Ticehurst & Veal, 2000; Stewart & Jürjens, 2018). These interviews aimed to refine variables, improve constructs, and enhance research tools for future quantitative research.

As interviews are socio-cultural constructs based on the participant's subjectivity, they require the researcher's attention to interpret their meanings. Although this process of interpretation is part of the data analysis, the interviewees' concerns were checked before the interview was recorded (Davidson, 2009). This practice is crucial in qualitative research to gather a complete set of accurate comments (Ticehurst & Veal, 2000). These precise comments make it possible to create constructs, measures, and definitions (Kvale & Brinkmann, 2009). Specific, pragmatic logic can be used in the transcription to facilitate the reader's understanding. For example, if the interviewee speaks very little, the words recorded on the tape are unlikely to be understood. Consequently, key informants have been informed of the situation in the transcription by the expression, as Marcuschi (2007) states.

During the interview process, the relationship between the interviewer and interviewee can greatly impact the conversation. In this study, the informants displayed a higher level of trust due to the rapport between them and the interviewer (Goudy & Potter, 1975; Lavin & Maynard, 2001). As a result, they were able to share their experiences in much greater detail. As the interaction continued, the respondents' main concern became the quality of the data being collected. However, their confidence in the researcher grew stronger and they showed a clear understanding of how their contribution would impact the study's findings. The researcher's ability to actively listen to the respondents was key in building and maintaining this relationship.

Due to the post-interview approach, there was an opportunity to collect post-interview data in all three cases. The conversations with interviewees continued to provide useful information and helped to recruit more key informants for follow-up interviews. This post-survey phase also provided access to additional data, such as company and audit reports (Blohm, 2007). This appreciation for the data

provided strengthened the relationship even more. For this reason, it is advisable not to switch off at the end of the survey but to remain alert for hints and signs of additional data opportunities. The analysis of the interviews presented here demonstrates that the relationship may continue beyond the initial interview.

The NVivo software (version 9) was used to analyse the interview, which met the research criteria by avoiding tedious transcription and improving the accuracy and efficiency of the analysis process. While qualitative data analysis programmes such as CAQDAS are not entirely error-free, NVivo software proved reliable (Wainwright & Russell, 2010; Bezeley, 2007; Walsh, 2003). The results of the interview analysis were used to develop the conceptual framework and research method for the quantitative analysis.

3.3.4. Observation

The observation methodology is based on a systematic approach. The researcher focused on various activities to draw attention to the diversity in this research (Angrosino & dePerez, 2000) and had the privilege of observing, partaking in a series of activities, and interacting with key informants throughout the lengthy process. Key informants explained the importance of the research to them personally and their intention to use the information to improve their current process. Building connections based on trust was crucial to encouraging informants to open up (Taylor & Bogdan, 1984; Merriam, 1998; DeWalt & DeWalt, 2002; Wolcott, 2001; Lincoln & Guba, 1994). Other best practices, such as ethical concerns, were addressed to minimise researcher bias and improve the effectiveness of the field experience (Angrosino & dePerez, 2000).

3.4. Quantitative Research Step

3.4.1. Overview

This section focuses on the quantitative research methodology, which follows the previous section, 3.3, on the qualitative research technique. First, this section presents how theory, measurement, and statistical evaluation levels are addressed and synchronised. The innovative nature of DT and the level of innovation incentives in the industries justify the measurement of organisations in the study of DT processes. Using a questionnaire survey as a means of data collection is explored, as well as the methods for ensuring that respondents have a common knowledge of the field context. The constructs are then initialised, considering the existing literature as well as the findings of the qualitative research. Finally, a rationale for the case selection is provided.

This chapter describes the quantitative analysis of the study conducted in the FinTech, financial sector, and automotive networks. Several processes had to be carried out before using confirmatory factor analysis and structural equation modelling to evaluate the hypothesis. First, the data were modified by recording, filling in gaps, and performing several tests, including a normality test. Second, the scales created were cleaned up in this post-processing phase.

3.4.2. Levels of Theory, Measurement and Statistical Evaluation

Cybersecurity must be consistent with theory at the industry level and the level of measurement and evaluation. Previous theories and analyses have focused on organisation or end-user as the only available level of measurement. Studies on DT have also neglected the security context, resulting in theories usually referring to technological innovations, digital products, and services (Arbanas & Hrustek, 2019; Luse et al., 2013; Samonas & Coss, 2014). As a result, measures, structures, and operational definitions are not associated with the level of security but with the organisational or relational level. To undertake innovative empirical IS security research to secure TD, these relative levels of theory, measurement, and statistical evaluation need to be defined to improve the rigour, precision, and clarity of the research to reduce the risk of fallibility (Klein et al., 1994).

The IS strategy and the cybersecurity level of DT constitute the theoretical level of this study. This research focuses on the theoretical level, which includes the degree of protection utilised for presentation and discussion and the stage at which broad strokes are drawn (Rousseau, 1985; Klein et al., 1994). This study focuses on the industries that provide digital products and services and the consumers who intend to adopt these digital products and services to improve cybersecurity in these two areas and extend beyond a sectoral perspective.

Rousseau's (1985) assertion, later cited by Klein et al. (1994), identifies the level of measurement as the specific unit that attributes the origin of a data set. When examining elusive and abstract phenomena, reducing to the lower unit level can be useful while focusing on the higher level of analysis (Yin, 2014, p. 45). The absence of empirical research and theory formation in IS security and DT security, and the preference for organisation-specific or relational studies, may be due to the abstract nature of the industries. The level of assessment of key informants from innovative organisations is considered appropriate in this study to promote verifiability. Multiple key informants within each organisation are interviewed to increase the credibility of their responses (Marsden, 1990b). These informants are more

concerned with security than with IS or DT. To focus on the case study investigation, Yin (2014) suggests considering the top level of analysis while measuring at the subunit level.

The analytical unit of the study is the inventive industries. Data processing in statistical techniques is clarified by the level of statistical analysis, as in the work of Klein et al. (1994). Given the number of informants interviewed, this data is grouped by industry and analysed at the industry level.

Briefly, the theoretical and analytical levels are industry-based, while measurement involves interviews with numerous key informants in each organisation, focusing on industry issues. Since industries are abstract, this serves to enable verifiability and tangibility. Despite differing aspects, the theoretical, measurement, and analytical levels lead to the industry level, allowing congruence.

3.4.3. Data Collection Method

A suitable technique for empirical testing of theoretical models is a questionnaire survey. This eases data quantification (Stewart & Jürjens, 2018; Stewart, 2022; Ticehurst & Veal, 2000). Theory development in this area would therefore benefit from quantification measures. Given the lack of industry constructs and measurements, the constructs and metrics described in this paper will significantly advance the field. In addition, the questionnaire survey applies to a wide range of industries due to its ease of replication, providing consistency of approach and the opportunity to duplicate its reliability (Blaxter et al., 2001).

The survey for this study was conducted using a hybrid approach that combined online, postal, telephone, and face-to-face methods (Walsham, 2006; Witmer et al., 1999). Based on their advantages and disadvantages, the researcher and management chose these techniques to minimise the potential drawbacks of survey research. Erroneous perceptions of the questionnaire's scope and low response and completion rates are the primary determinants of survey research (Kinnear et al., 1996). Due to the difficulty of delineating industries and abstraction, Kinnear et al. (1996) recommended verifying industry identification using input from a few reliable informants within the industry.

3.4.4. Questionnaire Design

Questionnaire design is complex because surveys can ask about topics at distinct information levels, questions can be asked in different ways, and questions asked at the beginning of a survey can influence their response to subsequent questions. Understanding how opinions or attitudes have been measured in previous surveys is crucial for researchers.

Therefore, following best practices for questionnaire development, the researcher and management set the objectives, resources, budget, and timeframe for the survey (Umbach, 2004). Doing so ensured that the sector was identified correctly (Perry & Rao, 2007). According to Ticehurst & Veal (2000), when conducting a questionnaire interview, it is essential to use the exact wording of the survey. If the respondent misunderstands the question, repeat the question and, if the misunderstanding persists, move on to the next question. This procedure is essential, as further explanation or elaboration could introduce bias.

To better understand how participants think about the subject or comprehend a question, pilot tests are conducted in this study during the initial stages of questionnaire construction. Pretesting is a crucial step in the production of questionnaires since it allows researchers to measure how respondents will respond to the entire survey and individual questions, mainly when posed for the first time. Based on extensive research in recent years, questionnaire design is not an art but a science that involves designing a good questionnaire. The questionnaires were then checked to see if they were necessary, how long, and if they contained all the information required for this study. Once the industry approved, the researcher conducted a pre-test and revised the questionnaire to get the final layout for approval by the industry. Once the final copy and layout of the questionnaire had been approved, it was time to complete the questionnaire, i.e., conduct the survey (Stewart, 2022). According to Cooper & Schindler (2006), Marsden (1990b), Wasserman & Faust (1995), and others, this hybrid approach to recognition and recruitment increases reliability by providing a common frame of reference. It allows flexibility in finding new organisations with common interests.

The hybrid technique reaches a broader audience, making the results more meaningful and credible, and eliminates previously known challenges of respondent misidentification leading to inconclusive results and low and incomplete response rates. The questionnaires were then assessed to determine whether they were necessary, how long they were, and if they provided all the information needed for this study. Following client acceptance, the researcher pretested and amended the questionnaire, resulting in the final questionnaire layout for client approval. After the final copy and layout of the questionnaire had been approved, it was time to field the questionnaire, i.e., conduct the survey. The questionnaires were divided into five parts: (i) introduction, (ii) preliminary screening of respondents, (iii) welcome questions (iv) progression to more detailed and subjective questions, and (v) closure (Stewart, 2022).

3.4.5. Scales and Measurement

The survey is divided into two portions, A and B, where A comprises demographic survey questions, whereas B comprises a five-level Likert-type scale (Ifinedo, 2014; Witherspoon et al., 2013; Kinnear et al., 1996), with each level having a value between 1 and 5. According to Cooper and Schindler (2006), different scales offer varying degrees of measurement concerning four characteristics: order, range, source, and classification. Ghauri & Gronhaug (2005) classified such scales as ratio, nominal, interval, and ordinal scales. There are normal scales at the lowest level of measurement, which provide numerical values based on categories or codes. Cooper & Chindler (2006) have argued that this classification remains elusive, even though they incorporate classification. Facility type, office type, industry, and location are used as control variables in this study using normal scales, while ordinal scales use the qualitative scale to classify the categories. Interval scales, on the other hand, use equidistant observations and a quantitative scale with arbitrary sources of information.

In contrast, ratio scales have an absolute origin but include quantitative scales with evenly spaced points (Blaxter et al., 2001). The Likert scale is an ordinal scale often used in questionnaires (Kinnear et al., 1996). For example, if a user has several items and uses a 5-point Likert scale, they should select 1-5 from the given responses. Churchill (1979) refers to it as a measure that maps specific structural properties. The Likert scale in this study is justified because it is simple and contains straightforward instructions (Kinnear et al., 1996). Although 7-tem and 3-tem scales have been used in other studies, a 5-tem scale was used in this study, which increased the precision and sensitivity of the measurements. In addition, the 5-tem Likert scale is easier to understand and use for survey officers and respondents. It requires less time and effort to complete than scales with higher scores. It offers choices to respondents without overwhelming them, and due to the sensitivity of the survey, item 5 was appropriate as it offers a deeper insight into respondents' thoughts and emotions.

3.4.6. Operationalisation of Constructs

This study uses Churchill's (1979) measurement construction method. This process consists of the subsequent steps: specifying the construct scope, creating an item sample, collecting data, cleaning the measurement, accessing reliability, assessing validity, and developing norms. The results of the qualitative interviews were combined with information from the existing literature in this phase. A list of metrics is proposed for each construct, building on previous metrics, and justifying emerging metrics.

3.5. Statistical Analysis

3.5.1. Overview

A quantitative pilot study and an extensive field study were conducted after pretesting the preliminary research instrument. Exploratory factor analysis and an internal reliability test were carried out to improve and assess the developed measures in the Finance industry as part of the pilot (Ticehurst & Veal, 2000). Extensive fieldwork was then conducted in FinTech, financial and automotive companies. Structural equation modelling is used in conjunction with confirmatory factor analysis at this stage. The research question addressed in this study is: What key factors can strengthen cybersecurity in DT, and how can they lead to effective security outcomes? These will be useful to highlight quantitatively the key elements and their influence on DT. Given that a case study design requires that the patterns within each industry are assessed and contrasted separately, survey results may not be replicable across industries (Yin, 2014).

Once trends emerge, the results can be extrapolated across the other two industries under consideration. Distinctions can yield industry-specific insights. Since quantitative empirical evidence at the cybersecurity and information security analysis level is lacking in both the IS and DT literature, quantitative analysis is beneficial to improve theory development. Lastly, given the critical significance of the scales developed for this study, tests of construct reliability, convergent, and discriminant validity will be conducted for them.

3.5.2. Exploratory Factor Analysis

As in the work of Churchill (1979), measures were purged using exploratory component analysis and coefficient alpha. Before conducting this analysis, the data are filtered by recording the relevant items and addressing missing data using the estimation maximisation method, recognized as preferable to its peer as it produces the most negligible bias (Hair et al., 2006; Kline, 2005). Unlike orthogonal rotation or other types of oblique rotation, such as quartimax rotation, varimax oblique rotation was applied in addition, resulting in more meaningful constructs with better factor discriminability, and is thus better suited to achieving the research goal of scale development (Hair et al., 2006). The SPSS was used during the EFA to examine the structure of the variables and confirm the dimensions identified in the exploratory interviews and addressed in the literature. Items with high correlations and excellent factor loadings reflected wider dimensions (Hair et al., 2006). At the initial stage of the exploratory research, a reliability value of 0.5 is acceptable (Nunnally, 1967). Chin (1998) proposed 0.6 or 0.5 as acceptable loadings if additional items related to the same factor have higher loadings. Cuieford (1965) and Hair et

al. (1998) recommended that Cronbach's alpha be greater than 0.7, although Hair et al. also suggested a rate of 0.6 in an exploratory study.

This research uses five logical processes in SEM: model design, identification, coefficients, model evaluation, and model modification (Kline, 2010; Hoyle, 2011; Byrne, 2013). Model specification yields the hypothesised relationships between variables in SEM based on one's expertise. The identification of the model determines whether it is overidentified, correctly identified, or misidentified. Model coefficients cannot be calculated for any model other than a recently identified or overidentified model. Model evaluation computes quantitative indices of the overall goodness of fit to assess the performance or fit of a model. Updating the model to improve model fit is called post-hoc model modification. Validation is the process of enhancing the reliability and robustness of the model.

3.5.3. Confirmatory Factor Analysis

There were several steps before using CFA with SEM to test the hypotheses. The data were first trained by re-coding, processing missing data, and performing random tests to determine if the data were normal. Second, in this post-fieldwork stage, the construct scales were refined. Third, validity and reliability analyses were conducted for all scales. Fourth, the fit of each construct to congeneric single-component models was evaluated. Fifth, a structural model was constructed using a single latent indicator variable, and the overall model fit was assessed. Hypothesis testing came after the fit was verified. After the fit was confirmed, hypothesis testing followed.

Scale refinement was performed using CFA in the post-survey stage after establishing normality. Although the CFA after the survey was considered appropriate because of the unique nature of the survey, the EFA was useful in the pilot phase in identifying the number of dimensions and their associated items. Given the unique nature of the study, EFA proved beneficial in determining the number of dimensions and associated items in the pilot phase; however, after fieldwork, CFA was deemed appropriate (Churchill, 1979). CFA conceptually justified its use at this level, given that only items relevant to specific dimensions are related to these factors, unlike EFA, where all items load on all factors, making it difficult to replicate the results (Cunningham, 2008; Gorsuch, 1983).

In addition, the CFA provides a measurement model that is related to the EFA but has none of the disadvantages of the EFA for biased research. It is conducted on the means and variance-covariance matrix rather than the correlation matrix. As a result, it can identify both non uniform and uniform bias.

In addition, since it is an inferential model, the model parameters can be evaluated statistically. CFA allows elegant structural, metric, and full equivalence modelling. Structural equivalence is maintained if the same factor model is used in each cultural group. This means that the expected factor loads significantly on each of the items. Metric equivalence is preserved if the factor loadings for each item are consistent across cultural groups. If factor loadings and axes are identical for each item, the full equivalence of scores is ensured. CFA is often used when many variables measure more than one dimension, as is EFA.

Thus, although items were omitted in the pilot data analysis to obtain an initial validity assessment, they remained in the entire survey because final removal was considered premature in the pilot data analysis. Given that the pilot study had a limited sample size within the financial sector, some items were likely to be more common in other sectors studied in the complete survey.

3.5.4. Structural Equation Modelling

The combination of structural equation modelling (SEM), confirmatory factor analysis (CFA), and path analysis have gained popularity as a statistical analysis approach for evaluating complete models (Byrne, 2001; Kline, 2005). In contrast to other multivariate techniques that consider only a single dependency relationship, SEM examines numerous relationships between independent and dependent variables (Hair et al., 2006). In addition, it provides goodness-of-fit assessments to measure the degree of support for the theoretical hypotheses presented (Cunningham, 2008). In addition, SEM has advantages because it includes measurement and structural uncertainty in its modelling, reflects unobserved terms, and produces more accurate estimates (Diamantopoulos, 1994). In contrast to other programs like Linear Structural Relationships (LISREL), Analysis of Moment Structures (AMOS) was selected for use in this study due to its compatibility with the SPSS statistical program, its ease of use and accessibility, and its efficient bootstrap approach for handling non-normal data (Cunningham, 2008; Arbuckle, 2006). This study analyses data from the complete survey using SEM and AMOS. SEM can evaluate complete models and provide accurate estimates that incorporate errors. SEM is widely accepted and easy to use.

3.6. Chapter Summary

This chapter provides a summary of the study's research design, including case studies, qualitative research, and quantitative research. Qualitative case studies and semi-structured interviews are justified, and case studies from the finance, fintech, and automotive industries are selected to support

pattern matching and future theory development. The first round of interviews explores and validates variables while identifying industries in detail. The second phase refines these areas and the research instrument. This also addresses the qualitative study's findings, and the conceptual model and hypotheses benefit from its input. Since there is a need for prior empirical studies in DT and IS cybersecurity, creativity is needed to contribute to theoretical strengthening. Key informants will assist with measurement, but theory, measurement, and statistical evaluation must be usable across industries. Identifying relevant industries involves initial questionnaires distributed through face-to-face interviews to reduce the possibility of misinterpretation of the framework of industries.

Qualitative research results are combined with existing literature to produce operational definitions and constructs. Statistical analysis uses an appropriate combination of factor analysis and SEM with pattern matching in case studies in selected industries. The constructs' reliability and validity successfully passed the test.

3.7. References

- Bezeley P. *Qualitative Data Analysis with NVivo*. London: Sage; 2007. [[Google Scholar](#)]
- Blohm, M. (2007), 'the influence of interviewers'' contact behavior on the contact and cooperation rate in face-to-face household surveys', *International Journal of Public Opinion Research*, 19 (1), pp.97-111.
- Creswell, J. W. (1998). *Qualitative inquiry and research design: Choosing among five traditions*. Sage Publications, Inc
- Creswell, J. W. (2010). *Projeto de pesquisa: métodos qualitativo, quantitativo e misto [Research design: Qualitative, quantitative, and mixed methods approaches]* (3rd ed). Trad. Magda Lopes, Rev. téc. Dirceu da Silva. Porto Alegre, Brazil: Artmed.
- Cully, M., Woodland, S., O'Reilly, A. and Dix, G. (1999), *Britain at Work: As Depicted by the 1998 Workplace Employee Relations Survey*. London, Routledge.
- Davidson, C. (2009). Transcription: Imperatives for qualitative research. *International Journal of Qualitative Methods*, 8, 1–52. <https://doi.org/10.1177/160940690900800206>
- Denzin, N., & Lincoln, Y. (2000). The discipline and practice of qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (pp. 1–32). Sage

- Eisenhardt, K. (1998), 'Building Theories from Case Study Research', *Academy Management Review*, Vol 14 (4), pp.532-550
- Goudy, W. J. and Potter, H. R. (1975), 'Interview Rapport: Demise of a Concept', *Public Opinion Quarterly*, 39 (4), pp.529-43
- Khalil, F., & Alam, H. M. (2020). Identification of Fintech Driven Operational RiskEvents. *Journal of the Research Society of Pakistan*, 1(57), 75–87
- Kvale, S., & Brinkmann, S. (2009). *Interviews: Learning the craft of qualitative research interviewing* (2nd ed.). London, United Kingdom: Sage
- Lavin, D and Maynard, D. (2001), 'Standardization vs. Rapport: Respondent Laughter and Interviewer Reaction during Telephone Surveys', *American Sociological Review*, 66 (3), pp.453-479
- Marcuschi, L. A. (2007). *Análise da conversação [Conversation analysis]* (6th ed.). São Paulo, Brazil: Ática.
- McAdam, R., Leonard, D., Henderson, J and Hazlett, S. (2008), 'A grounded theory research approach to building and testing TQM theory in operations management', *Omega*, 36 (5), pp.825-37.
- Patton, M. Q. (2002). *Qualitative research and evaluation methods* (3rd ed.). Thousand Oaks, CA: Sage.
- Wainwright M, Russell A. Using NVivo audio-coding: Practical, sensorial and epistemological considerations. *Soc Res Updat*. 2010. [December 9, 2014]. Available at: [google Scholar](#)
- Walsh M. Teaching Qualitative Analysis Using QSR NVivo. *Qual Rep*. 2003;8(2):251–256. [[Google Scholar](#)]
- Williams, A. (1968), 'Interviewer role performance: A further note on bias in the informant interview', *Public Opinion Quarterly*, 32 (2), pp.287-94.
- Yin, R. (2014). *Case Study Research: Design and Methods* (5th ed.). Thousand Oaks, CA: Sage Publications, Inc.

Chapter 4. STUDY I: Data security and consumer trust in FinTech innovation

Introduction

The first study, Data Security and Consumer Trust in Digital Innovations (e.g., Financial Technology), explores the impact of consumer response to DT, considering the mediating role of service quality expectations. Consumers who need more trust in digital products and services are often uncertain about where their data is stored, where it is transported and who has access to it. Typical indicators used to promote digital products and services, such as price and brand names, may not be appropriate quality indicators in these circumstances.

Furthermore, information technology (IT) and information systems (IS) are no longer seen merely as a support function for achieving strategic business goals but as an enabler that permeates the entire value chain of organisations (Hess et al., 2016). While technology was mainly integrated internally and used locally in the last century, it is now reshaping business processes, value chains and networks or redefining companies' scope through new business models (Veit et al., 2014; Venkatraman, 1994). In this constant flux, managers and leaders must continuously change to remain competitive, embrace new demands to adapt to them and invest in improving existing operational processes. They are constantly confronted with many potentially business-critical decisions.

While DT can improve users' daily activities and meet businesses' needs, the current sophistication of cybercrime can affect the quality of service before and during this innovation. This is an area that has not been sufficiently researched. One way to advance this area is through empirical research that explains the relationship between user and business behavioural intentions and the popularity of DT. Given the increasing number of data breaches that can result in penalties, fines and damages to a company, it is worth pursuing this line of research.

In addition, consumer response to the introduction of digital products and services may vary for experience and trust services. The way consumers respond to providing personal data online remains to be discovered.

Studies on decision-making under risk have revealed that human behaviour and choices often contradict the economic principle of utility axioms. This led to prospect theory's development and behavioural economics's emergence. Researchers from various fields have shown an increasing interest in the descriptive approach to understanding decision-making processes, which considers the limitations of information and constraints faced by decision-makers. Contextual factors also significantly influence decisions, and this is especially relevant in the rapidly changing and complex IS environment. Therefore, analysing decisions with a descriptive approach incorporating behavioural science insights can significantly benefit IS research.

To better understand the influences on the popularity of digital products and services, this study explores the reasons behind the challenges in adopting digital products and services.

Study I is presented in journal article format and published in the **Journal of Information and Computer Security by Emerald**. The presentation in this paper follows the format prescribed for the journal, while tables and figures have been placed throughout the article to facilitate reading. The paper is authored by Harrison Stewart and Jan Jürjens, with contributions corresponding to the contribution ratio for this article, which is set out on the next page.

<https://doi.org/10.1108/ICS-06-2017-0039>Statement of Authorship

CO-AUTHORSHIP APPROVALS FOR HDR THESIS EXAMINATION

PUBLICATION 1

This section is to be completed by the student and co-authors. If there are more than four co-authors (student plus 3 others), only the three co-authors with the most significant contributions are required to sign below.

Please note: A copy of this page will be provided to the Examiners.

Full Publication Details	Data security and consumer trust in FinTech innovation in Germany Stewart, H. and Jürjens, J. (2018), "Data security and consumer trust in FinTech innovation in Germany", Information and Computer Security, Vol. 26 No. 1, pp. 109-128. https://doi.org/10.1108/ICS-06-2017-0039									
Section of thesis where publication is referred to	Assistance with the comments of the journal editors (e.g. help with the clarity of the explanation of the results).									
Student's contribution to the publication	<table border="0" style="width: 100%;"> <tr> <td style="text-align: center; border-bottom: 1px solid black;">100</td> <td style="text-align: center;">%</td> <td>Research design</td> </tr> <tr> <td style="text-align: center; border-bottom: 1px solid black;">100</td> <td style="text-align: center;">%</td> <td>Data collection and analysis</td> </tr> <tr> <td style="text-align: center; border-bottom: 1px solid black;">99</td> <td style="text-align: center;">%</td> <td>Writing and editing</td> </tr> </table>	100	%	Research design	100	%	Data collection and analysis	99	%	Writing and editing
100	%	Research design								
100	%	Data collection and analysis								
99	%	Writing and editing								

Outline your (the student's) contribution to the publication:

Harrison Stewart designed the research, conducted data collection and analysed the data.
The text was written by him and I assisted him to revise some text to make it eligible for publication.

APPROVALS

By signing the section below, you confirm that the details above are an accurate record of the students contribution to the work.

Name of Co-Author 1 Jan Jürjens Signed  Date 12/12/27

STUDY I

Data security and consumer trust in FinTech innovation in Germany

Harrison Stewart, Jan Jürjens

Abstract

The advancement of mobile devices and their usage has increased the uptake of financial technology (FinTech) or financial technology innovation (FTI) in Germany. The financial sector and startups see FinTech as a gateway to increase business opportunities; however, mobile applications and other technology platforms must be launched to explore such opportunities. Mobile application security threats have increased tremendously and have become a challenge for both users and FinTech innovators. In this paper, we empirically consider factors that influence the expectations of both users and organizations in adopting FinTech, such as customer trust, data security, value added, the user design interface and FinTech promotion. The results confirm that customer trust, data security and the user design interface affect the adoption of FinTech. Our research proposes a model called "Intention to adopt FinTech in Germany," constructs of which were developed based on the Technology Acceptance Model (TAM) and five additional components, as identified. The outcomes of this study can be used to improve the performance of FinTech strategies and enable banks to achieve economies of scale for global intensity.

Keywords - FinTech, cyber security, mobile banking, data security, information security.

Paper type - Research paper

1.0. Introduction

A considerable amount of revenue has been invested in the information technology (IT) infrastructure of banks to enhance their performance, but investment in IT remains a substantial risk regarding the return on investment (Carlson, 2015). Most banks and financial organisations around the globe are subject to extreme pressure from their customers and competitors to enhance IT. In the 21st century, the main sources of revenue generation for German banks are interest margins and the provision of services such as wealth management, mortgage lending and financial advice. However, the benefit from these services has declined, causing many challenges for these banks as they strive to return to a period of profit. Today, most of these banks are embracing financial technology (FinTech), due to the promise of its ability to generate new revenue streams, personalize offers, target cross-selling and improve customer services. However, in order to explore such opportunities, mobile applications and other technology platforms need to be launched.

Germany has implemented various regulations and programs to encourage FinTech adoption; for example, during the Bundesbank 19th banking symposium, it was argued that banks in Germany need to adopt disruptive digital innovation to acquire technical awareness in advances (Patel, 2000; Stolterman & Fors, 2004). Furthermore, today's digital banking has broadened from standard online banking to inventive ideas that involve video consultancy services, credit brokerage and the incorporation of social media. The need for awareness of global cyber-attacks and their mitigation was also stressed.

Furthermore, cooperation between the Bundesbank, the BaFin, the European Banking Authority (EBA) and the European Central Bank (ECB) was suggested to establish an information technology audit service, with the intention of developing a supervisory regime to enhance security (Deutsche Bundesbank Eurosystem, 2015; Carlson, 2015). In the face of ongoing cyber-attacks, financial institutions must continue to strengthen their cyber security framework by investing assets in gathering, examining and sharing cyber-attack intelligence information to better comprehend the change in complex security risks (Carlson, 2015).

Cyber-attacks on FinTech services could bring about huge economic, social and organisational damage, which could also affect the trust of customers of these services (Kranz et al., 2013; Möller et al., 2012). The tremendous increase in mobile technology in Germany has increased mobile device convergence, internet and integration since 2013. In 2015, statistics gathered by ComScore demonstrated that 43.6

million humans use mobile devices to access social network platforms, online banking, emails and general internet usage; this figure is expected to rise to 58 million in 2018 (statista.com, 2015). Figure 1 demonstrates the adoption rate of mobile usage in Germany, which clearly shows its rapid expansion since 2013, making it a potential medium for the financial sector.

FinTech can be characterized as the utilization of mobile devices and other technology platforms to access a bank account, transaction notifications, and debit and credit alerts by means of push notification via APP, SMS or other forms of notification. It includes multi-banking features, block-chain, funds transfer, robot-advisory and concierge services from payments to wealth management, using mobile applications (Swift, 2010; Donner & Tellez, 2008). Cheney (2008) depicted such applications as "mobile financial services" and Datta (2011) described the advantages of mobile applications over standard online banking. Contrary to FinTech opportunities, the substantial security risk (Safa et al., 2015) has increased the need for information systems (IS) research regarding the quest for banks in Germany to establish a strategy for the successful adoption and implementation of FinTech innovation. Today, digital security is a bigger issue than it has ever been. Numerous prominent data breaches (Yeniman et al., 2011) over the past few years have resulted in a huge amount of lost income and have kept numerous banks from embracing FinTech. For example, in 2013, a cyber gang attacked more than 100 banking entities around the globe, which resulted in a total loss of \$1 billion to the banks (Kaspersky, 2015). This kind of attack is regarded as a Carbank attack (Kaspersky, 2015).

Several innovative banks have recognized the importance of security risk (Mannan & van Oorschot, 2007) and the barriers to the adoption of FinTech (Ndubisi & Sinti, 2006). In 2004, White and Nteli researched the barrier that security risk creates for digital banking in the UK and Australia. Poon (2008) argued the importance of security for individuals, regardless of age group, education or income. Subsequently, Manzano et al. (2009) researched the effects of security risk impacts on a bank account, a password and a customer's identity. Sonja and Rita (2008) also studied information risk, while Gerrard and Cunningham (2003) researched the outcomes of weak security measures and the ways that hackers

take advantage of this weakness. Phelps et al. (2000) studied the importance of privacy concerns and customer behaviour when it comes to providing personal information. Culnan (1993) focused on consumer conduct in the context of information usage. Similarly, Mahatanankoon et al. (2005) studied customer attitudes in the context of mobile applications, while Joubert and Belle (2013) researched

trust and risk in the context of mobile commerce adoption. Therefore, in this paper we raise the following questions:

1. What are the main inhibitors of FinTech innovation adoption?
2. Do customers prioritize FinTech value added over data security?
3. To what extent do data security and trust matter in the context of FinTech?

Due to the disregard of existing studies on the motivation for embracing FinTech in Germany, we intend to close the gap in the literature regarding this subject. This article analyses the key elements of customer trust, data security, value added, user design interface and promotion that influence FinTech services in Germany. Data security and trust play a central role in this regard, and we aim to consider them in the context of and in relationship to other aspects (such as usability), because we agree with other researchers who believe that these aspects should be considered together.

The first section has introduced the issues for this study and the research questions, while the second section gives a brief background of the issues. The third section provides a literature review on the topic, and the fourth section plots the motivation of our model, our research design and the hypothetical structure of this study. Our fifth section reports the empirical results and section six addresses the ramifications of the empirical key strategies to enhance FinTech in Germany. Section seven addresses the limitations of this study, and the last section outlines the paper's conclusions and future work.

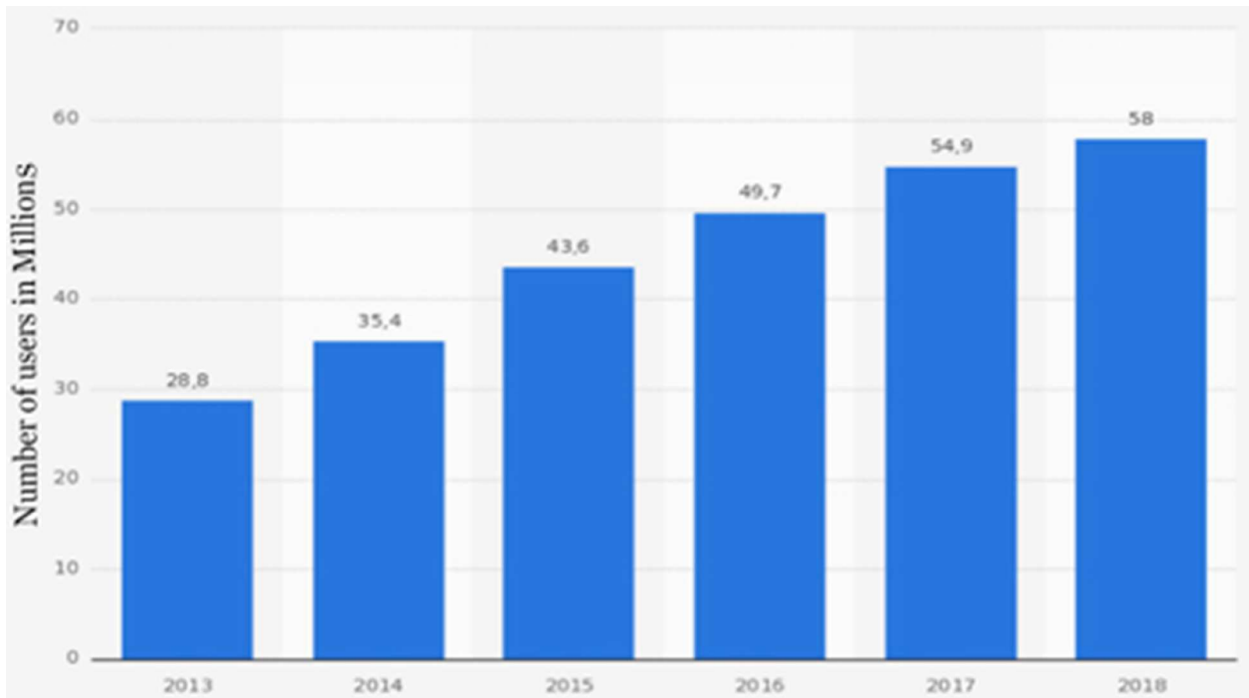


Figure-1: Total Number of Mobile Internet Users in Germany in 2013 and a Forecast to 2018

Source: <http://de.statista.com/statistik/daten/studie/180578/umfrage/anzahl-der-nutzer-des-mobilien-internets-in-deutschland-seit-2005>

2.0. Background

2.1 Concerns relating to FinTech data security.

As described in the international standard for information security management systems (ISO 27002), data security is the confidentiality, integrity, and availability of data. This is also known as the CIA triad (ISO/IEC 27002, 2013). The CIA triad has always been the business and industry standard in terms of data security; however, it is unsuitable for addressing the perpetually rapid dynamics of financial technology innovation. According to Whitman and Mattord (2009), data security is the insurance of both data and its crucial assets, e.g., the equipment in used for data gathering, data storage and the transmission process. Therefore, Whitman and Mattord (2009) included exactness, legitimacy, usefulness and ownership in data security measures. From a critical perspective, these varying definitions of data security require analysis. First and foremost, data protection should not be classified as an item or a product of technology, but rather as a process (Mitnick & Simon, 2002, p. 4). As indicated by Introna and Wood (2004), data security was previously considered technical; however, due to the massive utilization of both computers and networks today, data security must necessarily go

beyond the technical perspective. Safa et al. (2015) proposed information security awareness for better understanding, familiarity, and the capacity to manage and overcome crises. We also include human factor (Werlinger et al., 2009) in the data security definition, since FinTech organisation leaders and employees play a major role in securing data which will influence customers' trust in FinTech services.

2.2. Trust in FinTech

According to Lewis and Weigert (1985), trust is a complex, multidimensional phenomenon that plays a major part in business relationships. There are many elements that influence trust in FinTech innovation adoption, for example, data confidentiality, availability, integrity, constant wireless connection (Zhang & Lee, 2003), mobile application usability, transaction security, cultural influences and the trustworthiness of organisations (Whitman & Mattord, 2009; Siau et al., 2003). According to Joubert and Belle (2013), trust is essential in risky circumstances, and mobile applications come with numerous vulnerabilities that expose users to various risks. Furthermore, an essential component of trust is institution-based trust, which is an individual's belief that the platform they trade on is secure, as reported by Vance et al. (2008). Additionally, information security elements such as confidentiality, integrity, availability, authentication, accountability, assurance, privacy and authorization can essentially influence the beliefs and intentions of trust (Vance et al., 2008; Whitman & Mattord, 2009; Siau et al., 2003). Importantly, Vance et al. added that institution-based trust influences online platform trust. According to Vance et al. (2008), elements that determine system quality are applicable to the concept of trust, due to the technical aspects of information technology artefacts. In addition, Wang et al. (2003) elucidated solid support for the relationship between trust and usability. Specifically, usability enhances mobile-trade engagements and the trust impact in IT innovation.

3.0. Literature Review

Despite the substantial amount of research examining the process and techniques employed to effectively accept the adoption of FinTech, there is still the absence of a complete model to depict the disruptive FinTech innovation process in terms of data security and trust. Current innovation adoption theories and models must be modified and improved to highlight the perspectives necessary for the FinTech adoption process.

Ajzen and Fishbein (1980) proposed the Theory of Reasoned Action (TRA) to study the elements affecting an individual's conduct when embracing specific technologies. Specifically, TRA recognizes behaviour and subjective standards as the imperative indicators of an individual's intention to use a

specific technology. TRA suggests that an individual's behavioural intention is a combination of their attitude toward behaviour and subjective norm factors. In this model, an individual's performance of the behaviour is referred to as an attitude, as opposed to an individual's general performance (Fishbein & Ajzen, 1975). The subjective norm is the individual's recognition that humans who are beneficial to him/her think that he/she must or must not perform the behaviour being referred to. Therefore, TRA will not be appropriate for our study, since it foresees behaviour when the volitional control of individuals is violated (Ajzen, 1991). Furthermore, it lacks the ability to determine convictions which are pertinent to a specific behaviour.

Davis (1989) proposed the Technology Acceptance Model (TAM) that was later supported by Yang (2005) as the most robust model in the literature to study technology adoption designs. The fundamental objective of TAM was to declare factors which influence computer utilization. Accordingly, Davis took a few fundamental factors which were characterized as significant determinants of computer utilization in past studies and applied a psychological-based hypothesis – the Technology Acceptance Model (TAM) – for modelling and hypothesizing the connections among these factors (Davis et al., 1989). The TAM proposes that perceived usefulness (U), perceived ease of use (E), behaviour and usage influence a person's intention to use new technologies. Perceived usefulness is the degree to which individuals believe that utilizing a specific technology would upgrade their job performance. Perceived ease of use is the degree to which individuals believe that utilizing a specific technology would be free of effort (Davis, 1989). Simply put, as regards the TAM, it is believed that the utilization of a specific technology is influenced by intention to use, and intention to use this technology is determined by perceived usefulness and perceived ease of use. Therefore, Davis' study revealed that the relationship between usage and usefulness is more grounded than the relationship between ease of use (usability) and usage.

However, the validity of the measurement scales for TAM has also been scrutinized by other researchers. Ives and Olson (1984) and Venkatesh and Davis (2000) argued the deficiencies of the TRA, the TPB and the TAM. Furthermore, Straub et al. (1997) and McCoy et al. (2007) added that the TAM is not universally applicable and might not have the capacity to anticipate technology use in different cultures, since the model was developed in the United States. Venkatesh and Davis (2000) extended the TAM to TAM2 to eliminate the aforementioned limitations, by incorporating social impact and cognitive instrumental procedures as essential elements of information system adoption and usage, respectively. Luarn and Lin (2005) also argued that the TAM emphasises only U and E, and both tend to ignore the

constraints that hinder the utilization of information systems. Moreover, Liu et al. (2009) questioned the significance of TAM in the context of mobile banking services and highlighted the various impacts of the usage of computer-based systems and wireless-based systems. Luarn and Lin (2005) stressed the need for the advancement of the TAM to incorporate a trust element (perceived credibility) and two asset elements (perceived self-viability and perceived financial cost). They found that trust indirectly affects the customer's intention to adopt mobile banking based on E. Here, it is clear that awareness of inadequate data security measures for FinTech transactions among users equates to slower adoption of FinTech.

Tang et al. (2004) and Wang et al. (2003) contemplated the adoption of mobile banking by utilizing the TAM as a blueprint. They included customers' data security and protection concerns. Further, Luarn and Lin (2005) highlighted data security risks and data transmission concerns as vital elements that impact users adopting electronic conveyance channels. In addition, Clark (2002) and Lanford (2006) highlighted user design interface and usability as extra elements that need to be incorporated to address the data security concerns of users. As previously mentioned, the two distinct TAM constructs have been converged with the TRA model to form the value-added construct. Therefore, we explore the elements affecting FinTech in this study by extending the TAM to incorporate the components of data security and customer trust; we have excluded the unified theory of acceptance and use of technology (UTAUT) (Venkatesh et al., 2003) due to its complexity. Furthermore, UTAUT analyses the construct of social influences, which is not needed in the current work.

4.0. Methodology

Many studies, as examined in the literature section, have identified different factors which can impact the adoption of FinTech. As stated earlier, our work considered the variables or factors that would be more relevant for Germany, as well as factors in the TAM. The new model proposed has five factors, namely, data security, trust, value added, FinTech promotion and user design interface. We assume these are the factors that impact the behavioural intentions of customers in Germany to adopt FinTech services. The expanded TAM, as outlined in Figure 2, will be named the "Intention to adopt FinTech in Germany" model. In this study, the customers' acknowledgement of FinTech services is measured by their behavioural intention to utilize this innovation (Dillon & Morris, 1996; Tang et al., 2004; Sun, 2003). The decision to use the TAM as our research model to clarify customers' intention to adopt FinTech is attributed to its steady ability to clarify the changes between intentional behavioural and

actual behavioural (King & He, 2016). The five determinants that constitute the aforementioned research questions are shown in Table A.

In this paper, we empirically inspect the components that influence the expectations of both users and organisations to adopt FinTech, such as, customer trust, data security, value added, user interface design and FinTech promotion. Thus, security and trust play a central role in this work, and we aim to consider them in the context of, and in relationship to, other aspects (such as usability), because we agree with those researchers who believe that these aspects should be considered together.

4.1. Research design and theoretical framework

Based on our research, we grouped our methodology into two segments. In the first segment, we develop a theoretical framework based on the literature and information security hypothesis in this study. The second segment depicts the empirical framework used to analyse the key elements that improve the adoption of FinTech in Germany.

Table-A: Factors Impacting FinTech

Factors	Meaning
VA	Value added
CT	Customers' trust
DS	Data security
UI	User design interface
FP	FinTech Promotion

The internal and external elements that influence the adoption of FinTech are represented by the determinant value added (VA) in our model. The two main TAM constructs: U and E, represent the internal elements that determine the VA. In accordance with the TAM, U is the belief among individuals that they can be more productive by adjusting to a new technology (Lu et al., 2003), while E is the belief that the new technology is easy to use. In this context, customers will use the tool of interest in the event that they perceive it to be useful and free of effort. Thus, we have characterized our VA as any enhancement concerning the U, and the ability to better serve customers with less effort: E. In this manner, VA captures the TAM variables U and E as antecedents to the intention to use FinTech services. This can be compared to the TRA, due to the aggregation of effort and usability, but dissimilar to TAM,

where these two constructs are treated differently (Pikkarainen et al., 2004). The external factors of our VA are determined by the efficiency of secured telecommunication connectivity and coverage that gives customers simple and consistent access in embracing FinTech innovation (Venkatesh et al., 2003). In this paper, the connection speed of data transfer illustrates the motivation behind the intention to use FinTech (Carlsson et al., 2006). Various hypotheses were formed for testing, as summarized in Table B.

Table-B: Research Hypotheses in this Study

Ha	Customers' intention to adopt FinTech is not always influenced by the value added.	(Grazioli & Jarvenpaa, 2000) (Datta, 2011)
Hb	Trust does not always influence customer s' intention to adopt FinTech.	(Whitman & Mattord, 2009) (Yao et al., 2003)
Hc	The willingness of customers to trust FinTech is not influenced by data security.	(Amoroso & Hunsinger, 2009) (Joseph et al., 2012)
Hd	Data security does not influence customers' intention to adopt FinTech.	(Lee & Chung, 2009)
He	Customers' intention to adopt FinTech is not influenced by the user design interface.	(Lanford, 2006) (Laberge & Caird, 2000)
Hf	The user design interface does not influence the willingness of customers to adopt FinTech.	
Hg	Value added is not a vital determinant of trust in customers' intention to adopt FinTech.	(Pikkarainen et al., 2004) (Howcroft et al., 2002)
Moreover, financial institutions with rigid security measures (Kritzinger & vom Solms, 2010; Parker et al., 2015) should use promotion to promote their services. Along these lines, this study proposes the following theories:		
Hh	Promotion of FinTech services does not influence customers' intention to adopt FinTech.	
Hi	Promotion of FinTech services is not influenced by data security.	
Hj	Promotion of FinTech services is not influenced by the value added.	
Hk	Promotion of FinTech services is not influenced by the user design interface.	
Hi	Promotion of FinTech services does not influence trust in customers' intention to adopt FinTech.	

The above research analyses the previous links between the hypothetical constructs and variables. We illustrate these links in Figure.2. The hypothetical structure developed in our work aims to demonstrate that data security, trust, added value, user design interface and FinTech promotions are the conceivable antecedents for the adoption of FinTech in Germany. This gives refinements to existing hypotheses for FinTech adoption in Germany.

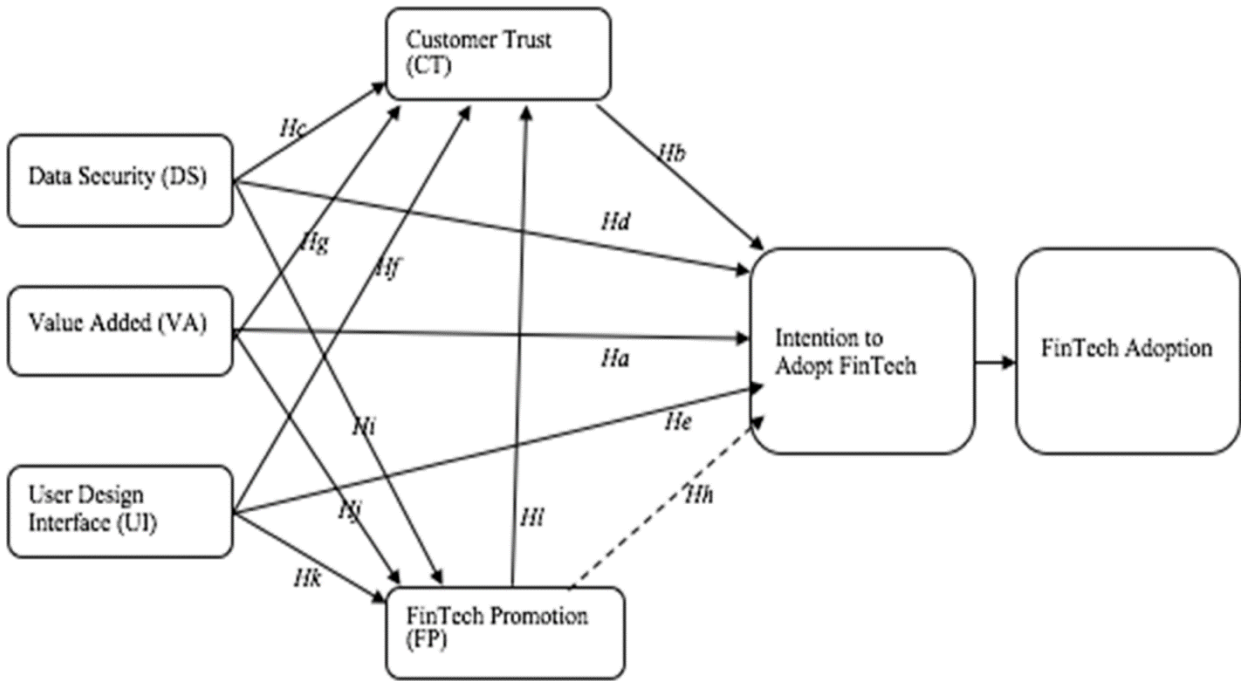


Figure-2: Proposed Research Model - Intention to Adopt FinTech in Germany

With the aid of the TAM and our testable hypothesis, we have been able to determine both the internal and external constructs that might determine FinTech adoption. However, at this time we cannot relate our hypothesis derived from our testable hypothesis to our research questions, due to the uncertainty of the results of our hypotheses and the competitive balance in our five determinants. At this point we can only assume that these five determinants might motivate and influence customers' intention to adopt FinTech.

5.0. Empirical Method

In this part of the research, we employed a quantitative methodology, with the goal of evaluating customers' perception with respect to data security concerns and trust in the intention to adopt FinTech services (Ashley & Boyd, 2006). A questionnaire survey was used to collect data. This methodology enables us to use numbers to clarify issues based on research conducted by Lundahl and

Skärvad (1992) and sum up the outcomes for the populace, as in the work of Burns and Grove (2001). Questionnaires were conducted through individual interviews and electronic email to bank customers in Germany. We distributed the questionnaires between August 8th and 14th, 2016. A questionnaire, consisting of 36 separate questions, was sent to 700 respondents. From this original sample, 308 completed questionnaires were returned. Of these, 99 questionnaires were discarded as unsatisfactory or redundant. The remaining 209 questionnaires were deemed to constitute an acceptable sample size - as they represent a 41.8% response rate. We used a stratified sampling design to choose our sample respondents. Table C illustrates the relation between the questions, variables and hypotheses.

Table-C: Survey Questions, Hypotheses, Variables

Meaning	Hypothesis	Questions
Data Security	Hd	Q4-Q16
Consumer Trust	Hc, He	Q17-Q22
Value Added	Ha, Hg	Q23-Q29
User Interface Design	Hf	Q30-Q35
FinTech Promotion	Hh, Hi, Hj, Hk, Hl	Q36

Data analysis was conducted with SPSS and AMOS. The analysis includes a validity test, descriptive statistical analysis, confirmatory analysis, exploratory factor analysis (EFA) and univariate analysis. This study attempts a three-phase approach. In the first phase, we analyse data utilizing EFA and a canonical correlation matrix for data decrements. A preparatory workshop for a pilot test disclosed the questions to participants and ensured that every participant understood the research motives. Here, 90 samples were used for the pilot test. We used EFA by employing the principal axis factoring technique on a Promax rotation to limit the items of every latent factor loaded. Every question was deciphered with different approaches to ensure that all participants understood all questions in the same way. We received five different eigenvalue factors that confirmed the five factors in the literature review and further tested their reliability with Cronbach's Alpha (Cuieford, 1965). Cronbach's Alpha is used to measure dependability of different Likert questions in a questionnaire that forms a scale (Allen & Yen, 2002; Bland & Altman, 1997; Cuieford, 1965). According to Cuieford, 0.7 of Cronbach's Alpha is high enough in an exploratory research test, and therefore researchers should target between 0.35 and 0.7 and discard all 41 values less than 0.35.

The second phase of the approach includes measurement model estimation employing confirmatory factor analysis (CFA). Here, the discriminant validity, reliability and convergence of our factors are converted to a data set of 199 samples. Thirdly, we used a structural equation model (SEM) that was derived from all models employed to test our hypothesis. In our work, the structural equation framework from the SPSS AMOS is used.

In this study, X_i signifies the latent variable that measures the intention of customers to adopt FinTech from the total respondents. The relationship that exists between X_i and an explanatory set of variables is indicated by r_i .

$$X_i = r_i' \beta + \varepsilon \quad (1)$$

The vector represents the elements that affect the adoption of fintech:

$$r_i' = [VA, CT, DS, UI, FP]'$$

The explanatory variables are exogenous and represent latent variables (V) measured by two or more perceived marker variables (Y). This then generates:

$$Y_i = L_v V + \varepsilon_v \quad (2)$$

Where

Y_i = The V vector of the marker

L_v = Loadings

V = Exogenous construct

ε_v = Measurement or estimation error h_i

Figure 2 represents a model to predict the perceived intention to adopt FinTech in Germany from the variables data security, customer trust, value added, user design interface and FinTech promotion, with the help of AMOS and the Statistical Package for Social Science (SPSS). We used the structural equation model (SEM) to test hypothesized relationships among our constructs and to validate the scientific behavioural approach of our study, as well as to estimate multiple correlations. This helped us to construct all our theories, which enabled us to present them with latent factors (Sadeghi & Hanzae, 2010).

5.1. Applying SEM

In general, we followed six basic steps. In the first step, also termed as model specification, we formulated the hypothesized relationships among the manifested variables (MV) and our latent variable (LV). Here we derived our relationships from current literature and past theories. As shown in Figure 2, our latent variable is depicted by “intention to adopt FinTech” and manifest variables (DS, CT, FP, UI and VA), shown by rectangles. The arrows display the hypothesized relationships, as shown in Figure 3. The next step was to identify our model (also known as model identification) in order to verify whether our model is appropriate for the degree of freedom we need to calculate. The degree of freedom of the model is ascertained by subtracting the number of parameters to be evaluated from the number of known components. According to Gefen et al. (2000), the model is over-identified if the degree of freedom is above zero. However, it was vital to make sure that our model would be over-identified, to enable us to analyse it.

The next step was to select the data that is needed for our work. This was very important, since SEM has issues with multicollinearity, sample size, missing data, normality and outliers. Several researchers have proposed that the minimum sample size should be 10, multiplied by the number of items during complex constructs (Gefen et al., 2000), while Weston et al. (2006) cited the work of Kline (1998) that 10 to 20 participants are needed per hypothesized relationships between two variables. Weston et al. (2006) proposed a standard sample size of 200 for SEM. Multicollinearity alludes to the circumstance where there is a solid relationship among measured variables ($r > 0.85$). In our work, we made sure to remove all items that might cause any multicollinearity (Weston et al., 2006). Since our work was focused only on Germany, we made sure to adhere to cases that were relevant in Germany, and classified cases that were not relevant to Germany as outliers. As per Field (2005), outliers allude to cases which are considered abnormal in relation to the main pattern of the data. Both outliers and missing data were removed from our data before we applied the SEM analysis, to prevent our model from being biased.

We then estimated our model by determining the value of obscure parameters and the error relationship with the estimation value. Here, we initially adopted confirmatory factor analysis to test the measurement model before we estimated the structural model, as in the work of Anderson and Gerbing (1988) and cited in Weston et al. (2006). We then evaluated our model (also known as model fit and interpretation). We then evaluated our fit based on the following: the strength and the significance of our hypothesized relationships, variance accounted for by our latent variables and origin (endogenous) observed, and how well our general model fits our observed data.

In general, SPSS, MS Excel and AMOS were used to analyse our data in this study. SPSS was used to conduct descriptive analysis, explanatory factor analysis, the normality test, the reliability test, outliers' detection and missing data detection. We saved our data in MS Excel and transmitted the data from SPSS to AMOS. Both our CFA and structural model analysis were done using AMOS.

6.0. Findings

In Figure 1, we demonstrated that the number of mobile users in Germany is rapidly increasing, yet the adoption of FinTech is extremely sluggish. It is intriguing to observe that 99% of respondents had mobile devices, but only 10% recognized FinTech. Further, it is significantly discouraging to perceive that only 10 out of the 209 respondents had ever used FinTech services, representing under 1% of the surveyed respondents. It is obvious that the FinTech incubators and banks offering FinTech services need to persuade their customers of the usefulness and value added advantages of FinTech.

This study has been conducted to determine the key factors that influence and provoke FinTech adoption. Our exploratory factors are data security (DS), customer trust (CT), user design interface (UI), value added (VA) and FinTech promotion (FP) (Robinson et al., 1991). We tested the discriminant validity, convergence and reliability of each variable, utilizing CFA. We illustrate these results in Tables D and E.

To determine customers' intention to adopt FinTech, we initiated several surveys to test our hypotheses. We set our Cronbach's Alpha to a rate higher than 0.7, based on standards set by Cuieford (1965) and Hair et al. (1998). Hair et al. added that a rate of 0.6 is acceptable in an exploratory study. As illustrated in Table E, the normal loading factor for the DS is 0.96 and the Cronbach's Alpha is 0.58, falling below both standards recommended by Cuieford (1965) and Hair et al. (1998). Normal loading factor is defined as a statistical method that represents correlations between items and factors (Tucker & MacCallum, 1993). The normal loading factor for the construct customer trust (CT) is 0.67, with a Cronbach's Alpha of 0.78. The normal loading factor for the construct value added (VA) is 0.58. with a Cronbach's Alpha of 0.94. The normal loading factor for the construct user design interface (UI) is 0.97, with a Cronbach's Alpha of 0.92. All our Cronbach's Alpha values are higher than 0.7 for all our constructs, apart from data security. In summary, based on confirmatory factor analysis, all the constructs tested in the EFA were important.

Next, we were able to summarize the factors that influence FinTech adoption as VA, CT, UI, and FP, and relate them to DS. Consequently, we conducted a fundamental diagnostic analysis for statistics,

exceptions and standards. We examined the convergent validity of our constructs by generating their average variances (AVE) (Farrell, 2009). AVE is a statistical tool defined as the average amount of variance in indicator variables that constructs are administered to define. Additionally, it has been recommended that AVE should surpass 0.5 for all constructs of a measurement framework (Cortina, 1993; Costello & Osborne, 2005). There was no critical deviation in the reported discoveries in the context of standards and exception.

We identify our suggested relationship model via SEM. Generally, the initial phase in SEM is to recognize the recommended suggestions of the relevant models, such as relative chi-squared (CMIN), comparative fit index (CFI), normed fit index (NFI), Tucker-Lewis Index (TLI), root mean square of approximation (RMSEA) and parsimony comparative fit index (PCFI). Figure 3 demonstrates that the SEM model fits our data best.

Table-D: Mobile Device Users and their Awareness of FinTech Survey Questions, Hypotheses, Variables

Mobile Device Users			FinTech Awareness	
	Frequency	%	Frequency	%
Yes	207	99	94	45
No	2	1	115	55
SUM	209	100	209	100

Table-E: Confirmatory Factor Analysis of Latent Reliability and Convergence Validity

Mobile Device Users			FinTech Awareness	
	Item	Normal Loading Factor	Cronbach's Alpha	Average Variance Extracted
Data Security (DS)	DS	0.96	0.58	0.68
Customer Trust (CS)	CT	0.67	0.78	0.47
Value Added (VA)	VA	0.58	0.94	0.54
User Design Interface	UI	0.97	0.92	0.93
Promotion (FP)	FP	0.74	0.86	0.48

[FP] FinTech Promotion [DS] Data Security [CT] Customer Trust [VA] Value Added [UI] User Design Interface

As stated earlier, our explanatory variables are exogenous and represent latent variables (V), which we measured by two or more perceived marker variables (Y) and grouped into items, as illustrated in Table E. Now we validate the discriminant validity of our confirmatory factor analysis, as illustrated in Table F.

Table-F: Confirmatory Factor Analysis of Discriminant Validity

FP	DS	CT	VA	UI	
0.478					FP
0.213	0.668				DS
0.056	0.350	0.025			CT
-0.111	0.26	0.098	0.34		VA
0.156	0.02	0.026	0.089	0.783	UI

[FP] FinTech Promotion [DS] Data Security [CT] Customer Trust [VA] Value Added [UI]

We now assess parsimonious indices that recommend that our model fits (PCFI = .84). Table G discoveries recommend that all calculated parameters in our hypothesis are essential. However, our CMIN is not exactly at the required cut-off value of 3.0, as recommended by Chau (1997). Here, our relative chi-square (CMIN) is $\chi^2/df = 1.83$, which is less than the required value. Our RMSEA is .06, which is appropriate, since it is between the 0.05 and 0.08 range recommended as a suitable model fit, as in the work of MacCallum et al. (1996). As in the work of Steenkamp and Van Trijp (1991) our comparative fit indices likewise show a model fit as follows:

(CFI = 0.98), (NFI = 0.91) and (TLI = 0.93).

Consequently, these observations conclude that our model fit the sample data in our work properly.

Table-G: Final Confirmatory Factor Analysis Model for our Model Fit

Fit Measures	Values Proposed	Values Observed
CMIN (χ^2/df)	≤ 3.0	1.79
Normed Fit Index	$\geq .90$	0.91
Parsimony adjusted to CFI	---	0.81
Tucker-Lewis Index	$\geq .90$	0.93
Comparative Fit Index	$\geq .90$	0.98
Root mean square error of approximation	$\leq .80$	0.05

After analysing our model fit, our empirical results indicate that the VA has much potential to influence the intention to adopt FinTech. UI also plays a major role in FinTech adoption. Here, our results indicate a 1% level of influence, and the empirical results illustrate that customers are more motivated to adopt FinTech when the user design interface is improved. The discoveries in this work verify that the effect of FinTech promotion does not have a direct or indirect impact on willingness of customers to trust FinTech.

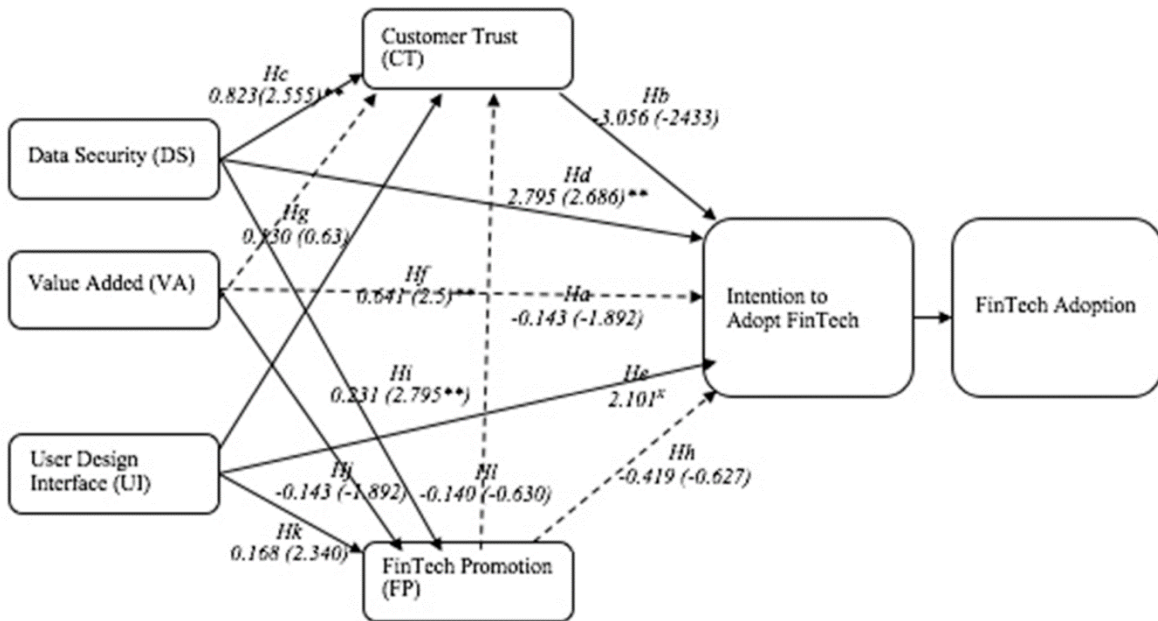


Figure-3: Proposed Research Model Fit - Intention to Adopt FinTech in Germany

Our standardized regression weight is based on y value, where **y < 0.01, *y < 0.05 .x path that had been fixed at 1.0 for model identification.

6.1. Univariate Analysis

Table-H: Univariate Analysis Results

	Hypothesis	Univariate Analysis
Hb	Trust does not always influence customers’ intention to adopt FinTech.	Rejected
Hc	The willingness of customers to trust FinTech is not influenced by data security.	Rejected

Hd	Data security does not influence customers' intention to adopt FinTech.	Rejected
He	Customers' intention to adopt FinTech is not influenced by user design interface.	Rejected
Hf	User design interface does not influence the willingness of customers to adopt FinTech.	Rejected

Based on the results generated in this study, as illustrated in Table H, there is sufficient evidence to reject Hb, Hc and He. Thus, we can deduce that data security and user design interface do influence customer trust, since there is a strong relationship between quality and trust. In the context of interface issues, Egger (2002) stressed attractiveness, perception and usability as vital factors of trust models. According to Donahue et al. (1999), usability is seen as a vital determinant of a smooth online trade. Kim and Moon (1998) also suggested that online commerce will win more trust than traditional commerce, due to the appeal of the web interface and its quality of information. Berger and Sasse (2001) argued that various interface factors can be clarified as trust, and Egger (2003) argued that customers are willing to explore websites that are relevant to them.

Moreover, Hc is rejected, since data security strongly influences customer trust, with approximately a 99% confidence level. In addition, the results fail to reject Hi, Hj, Hg and Hk. These indicate that data security, customer trust and user design interface do influence FinTech promotion. According to the results, Hb, Hc, Hd, He and Hf are all rejected at a 99% confidence level. Taken together, this implies that there is a hierarchy of important variables where data security, user design interface and customer trust are the principal components of customers' intention to adopt FinTech. However, the difference in mean score is small, particularly between user design interface and data security. It can then safely be concluded that all three constructs are influential over the intention to adopt FinTech.

For Hh, there is insufficient evidence to conclude that promotion influences the intention to adopt FinTech. Hl is also not rejected. This analysis answers our research questions regarding the primary hindrances of FinTech innovation adoption and what variables customers prioritize in the context of FinTech.

7.0. Limitations of the Study and Risk to Validity

There are a few limitations in this study. Initially, our study focuses on FinTech implementation in Germany and not the whole of Europe. In addition, demographic and regional factors could be consolidated to inspect their particular impact on the intention to use FinTech services, particularly among younger users with a high interest in technology. Without these constraints, we could have gathered additional data for a more robust result and obtained new knowledge to further upgrade policies to enhance the FinTech adoption process. Future analysts can assist exploration of this topic by altering determinants in the UTAUT model. Additionally, because the cluster sampling technique was used, the reported outcomes are not 100% generalized to the German population. To accomplish a complete generalization, a basic random sampling strategy for the whole population is essential. We could also alleviate some limitations by examining how online vendors are performing with regard to FinTech to satisfy the needs of customers via case studies.

This study was conducted in Germany and might have produced different results if held in other countries, since technology acceptance is different in a different environment. For instance, we suspect that the results would be somewhat different, were the research to be conducted in the United Kingdom, where take-up of FinTech appears to be far greater than in Germany. Therefore, our results are only generalized for the country of Germany and not other geographical areas.

Furthermore, respondents may have been influenced by past experiences about FinTech usage which might have led them to neglect to answer some questions. In spite of this, our study did not consider the influence of moderating variables such as age, education and FinTech services experience. We also neglected social impact and control factors, since their corresponding items disregarded the instrument dependability. Accordingly, we could not quantify social impact and control factors on FinTech use.

8.0. Conclusion

In this work, we empirically analysed the key factors, namely, customer trust (CT), data security (DS), value added (VA), user design interface (UI) and FinTech promotion (FP), that influence the intention to adopt FinTech, by using the TAM and Wang et al. (2003) model. Going beyond the standard TAM was indeed an important goal of this research to enable us to eliminate all the limitations that come with the TAM, by incorporating data security, trust, user interface and promotion as essential elements of FinTech adoption and usage. It was also vital for us to go beyond the standard TAM, since it only emphasizes perceived usefulness and perceived ease of use, and both tend to ignore the constraints that hinder FinTech adoption. The outcome, underpinned by statistical analysis, confirms that DS, CT

and UI are the solid foundation in FinTech adoption. Importantly, these three factors have critical impact on FinTech adoption, while DS significantly influences CT.

Based on our results, we can positively answer our first question with a strong argument that the principal hindrance to FinTech innovation are data security issues, poor user design interface and the absence of customers' trust. It is therefore essential that data security issues and the user design interface in FinTech need to be addressed effectively from the planning phase, to increase customers' confidence in FinTech. Examples have been given that delineate circumstances where information security and usability have been misjudged and discriminant validity has not been adequately evaluated or done well, which turns out to be a major hindrance in FinTech innovation. Customers' awareness of how data is being collected and used is still a major issue in the context of technology in Germany.

Consumers value their data and their privacy, and they have expectations. Today, through the media and social networks, customers are aware of the rapid increase of cyber-attacks on bank networks and data breach issues. Furthermore, they are also aware that little has been done by the industry to mitigate or prevent these attacks. Likewise, customers want to improve their standard of living, but are still cautious as regards the security of their data. They are disappointed when their essential data is intercepted by an unauthorized person or revealed to third-party companies. With respect to usability, customers are willing to explore products that are attractive and meet usability standards (Egger, 2002). According to Egger (2002) usability, attractiveness and perceptions are essential determinants of the trust model, and many other researchers have also stressed this (Egger, 2002; Donahue et al., 1999; Kim & Moon, 1998; Berger & Sasse, 2001; Egger, 2003). Furthermore, the increase in cyber-attacks on the wireless networks and operating systems of mobile banking platforms is still a major issue in the context of data security research. These attacks have brought about a high level of mistrust in the context of online payment transactions, due to the high risk of unapproved transactions from unauthorized persons.

It is obvious that the main deterrents to the adoption of FinTech are privacy and data security issues. It is therefore clear that such risks are more of a concern to customers than the quality of the product. It is also vital for financial institutions to enhance and sustain the CIA of customers' financial data and enhance the rules and legislation that accompany mobile applications (Yousafzai et al., 2005). In summary, the main hindrance to FinTech innovation adoption is data security, since this has a major influence on trust.

Our results also answer our second research question. Here, the current analysis demonstrates that perceived usefulness with respect to fraud protection and privacy has an immediate impact on the intention to adopt FinTech (Hoffman et al., 1999). Likewise, customers want to discover simple and strategic methods of preventing fraud and increasing the security of their data. In the context where customers feel safe and not threatened, their trust increases, and this thereby enhances their intention to adopt FinTech. This study reaffirms that data security has a strong influence on trust, but that value added, as any enhancement concerning the ability to better serve customers with less effort (U) and the belief that using FinTech would enhance customers' performance (perceived ease of use (E)), do not influence customers' intention to adopt FinTech. This indicates that customers do not prioritize value added over data security.

Our last research question is related to the extent that data security and trust matter in the context of FinTech. Here, we demonstrated that trust decreases the perception of risk in adopting FinTech, that is, there is a belief that an online company with a good reputation might provide secure encryption technologies and guarantees, should there be a dispute. All of these factors increase customers' trust and influence their desire to adopt FinTech services provided by a particular vendor.

The more customers are educated about and assured of their data being kept securely, the more their trust in financial technology will increase. It is therefore important that FinTech innovators understand customers' attitudes with regard to data and that they increase data transparency and security to enable customers' awareness of how data is being used and stored securely. Today, 82% of Germans are reluctant to share information with FinTech organisations, since they want to maintain their privacy (Statista, 2015). In a conjoint analysis survey, Germany was seen to be the country where humans placed the most value on their personal data, such as health data, credit cards, assets and government identities, when compared to the UK and the USA. We can therefore answer our third research question, that data security and trust matter greatly in FinTech adoption, and therefore FinTech innovators should enhance the security of their products and their online reputation in order to increase customers' trust. Customers can be educated and introduced to the advantages of FinTech, including its data security measures and benefits, through workshops, magazines, guidelines and consultancy.

Our study confirms that data security, customer trust and user design interface strongly affect the intention to adopt FinTech. These outcomes can be used to improve the performance of FinTech strategies and enable banks to accomplish economies of scale for global intensity. We hope that this

paper will serve to encourage FinTech innovators in their approach to this field, and enable FinTech researchers to make use of past work with more certainty, resulting in future hypothesis improvement.

References

- Ajzen, I. (1991), "The theory of planned behavior. Organisational Behavior and Human Decision Processes", 50, 179–211.
- Ajzen, I., & Fishbein, M. (1980), "Understanding attitudes and predicting social behaviour", Englewood Cliffs, NJ: Prentice Hall.
- Allen, M. J. & Yen, W. M. (2002), "Introduction to measurement theory". Long Grove, IL: Waveland Press.
- Amoroso, D. L. & Hunsinger, D. S. (2009), "Understanding consumers' acceptance of online purchasing". *Journal of Information Technology Management*, 10, 1, 15-41.
- Anderson, J. C. & Gerbing, D. C. (1988), "Structural equation modeling in practice: A review and recommended two-step approach". *Psychological Bulletin*, 103, 411- 423.
- Ashley, P. & Boyd, P. (2006), "Quantitative and qualitative approaches to research in environmental management". *Australasian Journal of Environmental Management*, 13, 70-78.
- Berger, J. R. & Sasse, M. A. (2001), "Trust builders and trustbusters: The role of trust cues in interface to e-commerce applications", available at:
www.cs.ucl.ac.uk/staff/J.Riegelsberger/trustbuilders_and_trustbusters.htm (Accessed 17 August 2016).
- Bland, J. M. & Altman, D. G. (1997), "Statistics notes: Cronbach's alpha". *BMJ*, 314 (7080):doi:
<http://dx.doi.org/10.1136/bmj.314.7080.572>.
- Burns, N. & Grove, S. K. (2001), "The practice of nursing research: Conduct, critique, and utilization". Philadelphia, PA: Saunders.
- Carlson, J. W. (2015), "Testimony on behalf of the Fin. Servs. Information Sharing & Analysis Ctr. ("FS-ISAC") Before the U.S. House of Rep", Comm. on Fin. Servs.
- Carlsson, C., Walden, P., & Bouwman, H. (2006), "Adoption of 3G+ services in Finland". *International Journal Mobile Communications*, 4, 369-385.

- Chau, P. Y .K. (1997), "Reexamining a model for evaluating information center success using a structural equation modeling approach", *Decision Sciences*, 28(2), 309-334.
doi:10.1111/j.1540-5915.1997.tb01313.x.
- Cheney, J. S. (2008), "An examination of m-banking and mobile payments": Building adoption as experience goods? (Discussion Paper 08-06). Philadelphia, PA: Federal Reserve Bank of Philadelphia, Payment Cards Center.
- Clark, L. (2002), "E- biz can be ruined by poor user interfaces", *Computer Weekly*, 5/23/2002, p18, 1p
Item: 7049855.
- Cortina, J. M. (1993), "What is Coefficient Alpha? An Examination of Theory and Applications". *Journal of Applied Psychology*, 78, 1, 98-107.
- Costello, A. B. & Osborne, J. W. (2005), "Best practices in exploratory factor analysis: Four recommendations for getting the most from your analysis". *Practical Assessment, Research and Evaluation*, 10, 7.
- Cuieford, J. P. (1965), "Fundamental statistics in psychology and education", 4th ed. New York, NY: McGraw-Hill.
- Culnan, M. J. (1993), "How did they get my name? An exploratory investigation of consumer attitudes Toward secondary information use". *MIS Quarterly*, 17, 341-363.
- Datta, P. A. (2011), "Preliminary study of ecommerce adoption in developing countries". *Information Systems Journal*, 21, 3-3.
- Davis, F. D. (1989), "Perceived usefulness, perceived ease of use, and user acceptance of information technology". *MIS Quarterly*, 13, 319-339.
- Deutsche Bundesbank Eurosystem. (2015), "Rapid increase in cyber risks", available at:
https://www.bundesbank.de/Redaktion/EN/Topics/2015/2015_07_08_rapid_increase_in_cyber_risks.html (Accessed 17 March 2016).
- Dillon, A. & Morris, M. G. (1996), "User acceptance of information technology: Theories and models". *Annual Review of Information Science and Technology*, 31, 3-32.

- Donahue, G. M., Weinschenk, S. & Nowicki, J. (1999), "Usability is good business", *Compuware Corporation Research Report*, available at:
<http://www.compuware.com/intelligence/articles/usability.htm> (Accessed 17 August 2016).
- Donner, J. & Tellez, C. A. (2008), "Mobile banking and economic development: Linking adoption, impact, and use". *Asian Journal of Communication*, 18, 318-322.
- Egger, F. N. (2002), "Consumer trust in E-Commerce: From psychology to interaction design". In: J. E. J. Prins, et al. (Eds.). *Trust in Electronic Commerce: The Role of Trust from a Legal, an Organisational and a Technical Point of View*. Kluwer Law International.
- Egger, F. N. (2003), "Fromito Transactions: Designing the trust experience for business-to- consumer electronic com", available at: <http://www.ecommuse.com> (Accessed 17 August 2016).
- Farrell, A. M. (2009), "Insufficient discriminant validity: A comment on Bove, Pervan, Beatty and Shiu". *Journal of Business Research*, 63, 324-327.
- Field, A. (2005), "Discovering statistics using SPSS", London, UK: Sage Publications.
- Fishbein, M., & Ajzen, I. (1975), "Belief Attitude, Intention and Behavior: And Introduction to theory and Research. Reading, MA: Addison-Wesley.
- Gefen, D., Straub, D. W. & Boudreau, M.-C. (2000), "Structural equation modeling and regression: Guidelines for research practice". *Communications of AIS*, 4,7, 1-80.
- Gerrard, P. & Cunningham, J. B. (2003), "The diffusion of internet banking among Singapore consumers". *International Journal of Bank Marketing*, 21, 1, 16-28.
- Grazioli, S. & Jarvenpaa, S. L. (2000), "Perils of internet fraud: An empirical investigation of deception and trust with experienced internet consumers". *IEEE Transactions on Systems, Man and Cybernetics Part A: Systems and Human*, 30, 395-410.
- Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998), "Multivariate analysis", 5th ed., Englewood Cliffs, NJ: Prentice Hall International.
- Hoffman, D. L., Novak, T. P., & Peralta, M. A. (1999), "Building consumer trust online". *Communications of the ACM*, 42, 80-85.

- Howcroft, B., Hamilton, R., & Hewer, P. (2002), "Consumer attitude and the usage and adoption of home-based banking in the United Kingdom". *International Journal of Bank Marketing*, 20, 111-121.
- Introna, L. D. & Wood, D. (2004), "Picturing algorithmic surveillance: The politics of facial recognition systems". *Surveillance & Society*, 2, 177-198.
- Ives, B. and Olson, M.H. (1984), "User involvement and MIS success: A review of research", *Management Science*, 30.5, 586-603.
- ISO/IEC 27002:2013 "Information technology - Security techniques - Code of practice for information security controls", 2nd ed., available at: <http://www.iso27001security.com/html/27002.html> (Accessed 9 March 2016).
- Joseph, D. B. et al. (2012), "An analysis of web privacy policies across industries [interactive]", Worcester Polytechnic Institute, available at: https://www.wpi.edu/Pubs/E-project/Available/E-project-121412-121246/unrestricted/IQ_Final_Report.pdf (Accessed on 10 June 2016).
- Joubert, J. & Belle, J.-P. (2013), "The role of trust and risk in mobile commerce adoption within South Africa". *International Journal of Business, Humanities and Technology*, 3, 27- 38.
- Kaspersky Lab, Carbank Apt The Great Bank Robbery, Version 2.1 4 (2015), available at: <http://www.kaspersky.com/about/news/virus/2015/Carbanak-cybergang-steals-1-bn-USDfrom-100-financial-institutions-worldwide> (Accessed on 10 August 2016).
- Kim, J. & Moon, J. Y. (1998), "Designing towards emotional usability in customer interfaces Trustworthiness of cyber-banking system interfaces". *Interacting with Computers*, 10, 1, 1-29.
- King, W. R. & He, J. (2016), "A meta-analysis of the technology acceptance model". *Information & Management*, 43, 740-755
- Kline, R. B. (1998), "Principles and practice of structural equation modeling". New York, NY: Guilford.
- Kranz, M., Murmann, L., & Michahelles, F. (2013), "Research in the large: Challenges for large-scale mobile application research: A case study about NFC adoption using gamification via an app store". *IJMHCI*5(1), 45-61. doi:10.4018/jmhci.2013010103.

- Kritzinger, E. & von Solms, S. H. (2010), "Cyber security for home users: A new way of protection through awareness enforcement". *Computers & Security*, 29, 8, 840-7.
<http://dx.doi.org/10.1016/j.cose.2010.08.001>.
- Laberge, J. & Caird, J. K. (2000), "Trusting the online banking interface: Development of a conceptual model relevant to E-commerce transactions." Paper presented at the workshop Designing Interactive Systems for 1-to-1 Ecommerce at the ACM SIG CHI Conference, The Hague, the Netherlands.
- Lanford, P. (2006), "E-commerce: A trust perspective. Proceedings of the 2006 International Conference on Semantic Web & Web Services", the 2006 World Congress in Computer Science, Computer Engineering, and Applied Computing, Las Vegas, NV.
- Lee, K. C. & Chung, N. (2009), "Understanding factors affecting trust in and satisfaction with mobile banking in Korea: A modified DeLone and McLean's model perspective". *Interacting with Computers*, 21, 5/6, 385-392.
- Lewis, J. & Weigert, A. (1985), "Trust as a social reality". *Social Forces*, 63, 967-985.
- Liu, Z., Min, Q., & Ji, S. (2009), "An empirical study on m-banking adoption": The role of trust. In Proceedings of the 2009 Second international Symposium on Electronic Commerce and Security, Nanchang, China.
- Luarn, P. & Lin, H. H. (2005), "Toward an understanding of the behavioural intention to use mobile banking". *Computers in Human Behaviour*, 21, 873-891.
- Lundahl, U. & Skärvad, P. H. (1992), "Utredningsmetodik för samhällsvetare och ekonomer", 2nd edition. Sweden: Student litteratur.
- MacCallum, R.C., Browne, M.W., Sugawara, H.M. (1996), "Power Analysis and Determination of Sample Size for Covariance Structure Modeling ", *Psychological Methods*, 1:130-49.
- Mahatanankoon, P. et al. (2005), "Consumer-based m-commerce: Exploring consumer perception of mobile applications". *Computer Standards & Interfaces*, 27, 347-357.
- Mannan, M. & van Oorschot, P. C. (2007), "Security and usability: The gap in real-world online banking", In: Proceedings of the 2007 New Security Paradigms Workshop. New Hampshire, USA.

- Manzano, J. A., Navarre, C. L., Mafe, C. R., & Blas, S. S. (2009), "Key drivers of internet banking service use". *Online Information Review*, 33, 672-695.
- McCoy, S., Galletta, F., & King, R. (2007), "Applying TAM across cultures: The need for caution". *European Journal of Information Systems*, 16, 81-90.
- Mitnick, K. & Simon, W. L. (2002), "The art of deception: Controlling the human element of security", New York, NY: John Wiley & Sons.
- Möller, A., Michahelles, F., Diewald, S., Roalter, L., & Kranz, M. (2012), "U Kranz pdate behaviour in app markets and security implications: A case study in Google play", In: Poppinga B. (ed.), *Proceedings of the 3rd International Workshop on Research in the Large*, held in Conjunction with Mobile HCI, pp. 3-6.
- Ndubisi, N. O. & Sinti, Q. (2006), "Customer attitudes, system's characteristics and internet banking Malaysian". *Management Research News*, 29, 16-27.
- Parker, F., Ophoff, J., Van Belle, J. P., & Karia, R. (2015), "Security awareness and adoption of security controls by smartphone users", *Second International Conference on Information Security and Cyber Forensics (InfoSec)*, Cape Town, South Africa, pp. 99-104.
- Patel, K., McCarthy, M. P., Chambers, J. (2000), "Digital transformation: the essentials of ebusiness leadership", New York.
- Phelps, J. et al. (2000), "Privacy concerns and consumer willingness to provide personal Information". *Journal of Public Policy and Marketing*, 19, 27-41.
- Pikkarainen, T., Pikkarainen, K., Karjaluoto, H., & Pahnla, S. (2004), "Consumer acceptance of online banking: An extension of the technology acceptance model". *Internet Research*, 14, 224-235.
- Poon, W. C. (2008), "Users' adoption of e-banking services: The Malaysian Perspective". *Journal of Business & Industrial Marketing*, 21, 59-69.
- Robinson, J.P, Shaver, P. R., & Wrightsman, L. S., (Eds.). (1991), "Measures of personality and social psychological attitudes (pp. 1-15). San Diego, CA: Academic Press.
- Sadeghi, T. & Hanzae, H. K. (2010), "Customer satisfaction factors (CSFs) with online banking services in an Islamic country: I.R. Iran". *Journal of Islamic Marketing*, 1, 3, 249-267.

- Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan T. (2015), "Information security conscious care behaviour formation in organisations". *Computers & Security*, 53, 65-78. <http://dx.doi.org/10.1016/j.cose.2015.05.012>.
- Siau, K. et al. (2003), "Development of a framework for trust in mobile commerce", Proceedings of the Second Annual Workshop on HCI Research in MIS", Washington: Seattle, pp. 85-89.
- Sonja, G. K. & Rita, F. (2008), "Consumer acceptance of internet banking: The influence of internet trust". *International Journal of Banking Marketing*, 26, 483-504.
- Statista.com, (2015). Prognose zur anzahl der nutzer des mobilen internets in Deutschland bis 2019, available at: <http://de.statista.com/statistik/daten/studie/180578/umfrage/anzahl-der-nutzer-des-mobilen-internets-in-deutschland-seit-200> (Accessed 30 August 2016).
- Stolterman, E. & Fors, A. C. (2004), "Information technology and the good life", In *Information Systems Research: Relevant Theory and Informed Practice*, p. 689.
- Sun, H. (2003), "An integrative analysis of TAM: Toward a deeper understanding of technology acceptance model", In: Proceedings of the 9th American Conference on Information Systems, p. 2255.
- Steenkamp, J. E. M. & Van Trijp, H. C. M. (1991), "The use of LISREL in validating marketing constructs". *International Journal of Research in Marketing*, 8, 283-299.
- Straub, D., Keil, M., & Brenner, W. (1997), "Testing the technology acceptance model across cultures: A three country study". *Information and Management*, 33, 1-11.
- Swift. Mobile payments (2010). Technical report, *Swift White Paper*.
- Tang, T. I., Lin, H. H., Wang, Y. S., & Wang, Y. M. (2004), "Toward an understanding of the behavioural intention to use mobile banking services", PACIS 2004 Proceedings, 131, <http://aisel.aisnet.org/pacis2004/131>
- Tucker, L. & MacCallum R. (1993), "Exploratory factor analysis: A book manuscript, available at: <http://www.unc.edu/~rcm/book/factornew.htm> (Accessed 3 August 2016).
- Vance, A. et al. (2008), "Examining trust in information technology artifacts: The effects of system quality and culture". *Journal of Management Information Systems*, 24, 3-100.

- Venkatesh, V. & Davis, F. D. (2000), "A theoretical extension of the technology acceptance model: Four longitudinal field studies". *Management Science*, 45, 186-204.
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003), "User acceptance of information technology: Toward a unified view". *MIS Quarterly*, 27, 186-204.
- Wang, Y. S., Wang, Y. M., Lin, H. H., & Tang, T. I. (2003), "Determinants of user acceptance of internet banking: An empirical study". *International Journal of Service Industry Management*, 14, 501-519.
- Werlinger, R., Hawkey, K., Beznosov, K. (2009), "An integrated view of human, organisational, and technological challenges of IT security management", *Information Management & Computer Security*, 17, 4-19, available at: 10.1108/09685220910944722 (Accessed 13 August 2016).
- Weston, R., Paul, A. & Gore, J. (2006), "A brief guide to structural equation modeling". *The Counseling Psychologist*, 34, 5, 719-751.
- White, H. & Nteli, F. (2004), "Internet banking in the UK: Why are there not more customers?" *Journal of Financial Services Marketing*, 9, 49-56.
- Whitman, M., & Mattord, H. (2009), "Principles of information security (3rd ed.). Boston, MA: Course Technology.
- Yao, J. E., Lu, J., Yu, C. S., Liu, C. (2003), "Technology acceptance model for wireless Internet". *Internet Research*, 13, 206-222.
- Yang, K.C. (2005), "Exploring factors affecting the adoption of mobile commerce in Singapore", *Telematics and Informatics*, 22, 257-277.
- Yeniman, Y., Ebru .G., Aytac, S. & Bayram, N. (2011), "Factors influencing information security management in small-and medium-sized enterprises: A case study from Turkey". *International Journal of Information Management*, 31, 360-365.
- Yousafzai, S. Y., Pallister, J. G. & Foxall, G. R. (2005), "Strategies for building and communicating trust in electronic banking: A field experiment". *Psychology and Marketing*, 22, 181-201.
- Zhang, Y., Lee, W. & Huang, Y. A. (2003), "Intrusion detection techniques for mobile wireless networks". *Wireless Networks*, 9, 545-556.

CONCLUSION TO STUDY I

**Data security and consumer trust in FinTech
innovation**

The first study in this thesis provided evidence that disruptive technologies (DT) can be used as an extrinsic proxy to influence consumers' quality expectations of a service offering, influencing their intention and willingness to adopt DT services and products. These findings have thus answered the research questions posed in Chapter 1 to the hypotheses on the use of the belief that digital products and services are influenced by data security, trust and value-added. The results show that data security certainty and trust increase humans's intention to use digital products and services. In addition, digital product and service promotion and interface do not significantly influence the intention to use DT.

The results suggested that companies that are implementing or planning digital innovations need to address the issue of security seriously to gain customers' trust, which in turn impacts their willingness to adopt the innovation. The findings also suggested that due to the speed and competition in the competitive market, data security has been neglected, and the focus has been more on usability, design interface and promotion.

As the impact of security and its influence on the intention to adopt DT underlies customer expectations, data security and trust have a major impact on customers, especially in countries where data security and privacy, such as the GDPR, are mandatory and taken seriously. Companies planning to move away from their traditional products and services need to address the issue of security from the onset and ensure its sustainability.

Study II, therefore, explored how organisations offering digital products and services or planning to do so perceive digital services themselves. In today's cloud migration, high demand and scalability are forcing organisations to move to the cloud to focus their workforce on services and products and to reduce the burden of infrastructure management and security. In addition, the cloud infrastructure perceived by enterprises such as IaaS, PaaS and SaaS can be influenced by how the cloud provider can assure them of the security and protection of their critical information. In addition, Study II examines the impact of data security, trust and privacy on cloud migration adoption. Therefore, Study II examines perceived cloud adoption to probe the key constructs that influence cloud migration adoption.

Study 2 is presented in the next chapter.

Chapter 5. STUDY 2: The hindrance of cloud computing acceptance within the financial sectors in Germany

Introduction

The second study, "The hindrance of cloud computing acceptance within the financial sectors in Germany" (e.g., Infrastructure as a Service), extends study 1. The aim of study 2 is to explore the challenges of cloud migration and the combination of constructs that can improve this adoption, considering data security, trust and other constructs - as critical constructs that influence the perception of DT.

Information systems (IS) and information technology (IT) are no longer just strategic business objectives but a factor that permeates the entire value chain of a company (Hess et al., 2016). Corporate processes, value creation and networking, are currently being transformed by technology. It is also changing the scope of action of organisations through new business models. In the previous century, technology was mainly used domestically and at the regional level (Veit et al., 2014; Venkatraman, 1994). To remain competitive, organisations must embrace and adapt to new opportunities and invest in strengthening their core processes as they are constantly confronted with mission-critical business decisions.

As consumers become more sophisticated about digital products and services, they become more sceptical about data security and trust (e.g., Stewart, 2022). Consumers' perceived security and trust can impact their acceptance and adoption of digital products and services. Likely, the data and information security perceived by companies and their customers will influence their use of the DT.

To better understand the influences on the popularity of cloud acceptance, this study aims to explore the reasons behind the challenges in adopting cloud services.

Study 2 is presented in journal article format and published in the **Journal of Information and Computer Security by Emerald**. The paper's presentation adheres to the journal's guidelines, and tables and figures have been inserted strategically to make reading easier. Harrison Stewart is the only author of the article.

<https://doi.org/10.1108/ICS-01-2021-0002>

Statement of Authorship

CO-AUTHORSHIP APPROVALS FOR HDR THESIS EXAMINATION

PUBLICATION 2

This section is to be completed by the student and co-authors. If there are more than four co-authors (student plus 3 others), only the three co-authors with the most significant contributions are required to sign below.

Please note: A copy of this page will be provided to the Examiners.

Full Publication Details	The hindrance of cloud computing acceptance within the financial sectors in Germany Stewart, H. (2022), "The hindrance of cloud computing acceptance within the financial sectors in Germany", Information and Computer Security, Vol. 30 No. 2, pp. 206-224. https://doi.org/10.1108/ICS-01-2021-0002
Section of thesis where publication is referred to	All

Student's contribution to the publication	100 %	Research design
	100 %	Data collection and analysis
	100 %	Writing and editing

Outline your (the student's) contribution to the publication:

Harrison Stewart is the sole owner of this publication.

APPROVALS

By signing the section below, you confirm that the details above are an accurate record of the students contribution to the work.

Name of Co-Author 1 _____	Signed _____	Date _____
Name of Co-Author 2 _____	Signed _____	Date _____

STUDY 2

The hindrance of cloud computing acceptance within the financial sectors in Germany

Harrison Stewart

Abstract

Cloud computing offers a variety of potential benefits for large retail banks, including scalability, elasticity, high performance, resilience and security, and cost efficiency. A key challenge is understanding and managing the risks associated with the adoption and integration of cloud computing capabilities in the banking sectors. Effectively managing the security and resiliency issues associated with cloud computing capabilities is causing many banks in Germany to renew, and in some cases rethink, their processes for assessing risk and making informed decisions related to this new model of service delivery. This study attempts to find these challenges and propose factors to overcome the existing problems. To identify the various challenges, the study proposes a specific model called "IaaS Adoption". The model was validated through an online survey of 208 bank employees. The Partial Least Squares (PLS-SEM) led to the validation of the proposed model

Keywords - Finance, cloud migration, cloud computing, IaaS, IaaS, data security, TAM, TOE

Paper type - Research paper

1.0. Introduction

NIST defines cloud computing as the provision of on-demand computing services over the Internet to deliver rapid innovation, agile resources, and economies of scale. This cloud computing model has three service models, and four deployment models. The four deployment models are: public, private, hybrid and community. All of these models are associated with three integration (service) models, namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS)

(Modi et al., 2012; Coppolino et al., 2016; Ramachandran, 2015). Each of these deliveries and models brings its own challenges in terms of risk exposure. (i) A private cloud is operated by a specific cloud user, (ii) a public cloud is operated and run by the cloud provider, but leased to cloud users, (iii) a community cloud is used by organisations that collaborate and share the same goals, and (iv) a hybrid cloud is a combination of private and/or public clouds that provide a higher level of adaptability, availability, security and privacy (Armbrust et al., 2010; Suthaharan & Panchagnula, 2012; Sari, 2015). Cloud infrastructure and on-premise infrastructure are subject to the same threats (Al-shqeerat et al., 2017; Djemame, 2016; Nada et al., 2017; Rot, 2017, Wang, 2017). With the increasing number of cloud users per day, the amount of data stored by cloud providers is growing rapidly and has emerged as an attractive target for attackers. The three most common cloud infrastructure models are the IaaS, PaaS and the SaaS. In the IaaS model, a cloud user exploits the computing, storage or network infrastructure. In PaaS, a cloud user uses the sources provided by the cloud provider to run the various applications, and in SaaS, a cloud user uses software applications that run on the cloud provider's infrastructure.

In this paper, we attempt to present a comprehensive study of data protection in the IaaS environment; a major concern that requires ensuring consistency and security of data in transmission and access to and from the cloud, and scaling resources up and down. Despite a number of studies on the benefits, challenges and adoption of cloud computing, the IaaS rate still faces several critics, so it is important to address these challenges and identify the factors that are hindering the adoption of IaaS by banks in Germany (Gholami & Laure, 2015; Chou, 2013; Kozlov et al., 2018; Esposito & Castiglione, 2017; Armbrust et al., 2009; Mostajeran et al., 2017; Belbergui, 2017; Lee, 2012; Al-shqeerat et al., 2017). The risk of IaaS includes the risk of damage, injury, liability, loss or other adverse events caused by external or internal vulnerabilities and therefore this paper raises the following questions:

1. What is the connection between the factors that cause the challenges in the IaaS implementation model at banks in Germany?
2. Can data security and consumer trust help improve the performance of IaaS strategies and enable banks to achieve economies of scale for global intensity?
3. To what extent are data security and consumer trust important in the context of IaaS?

In the first section, the adoption to this study and the research questions were presented, while the second section provides a literature review on the topic and the third section introduces the motivation behind our model, our research design and the hypothetical structure of this study. The fourth section reports on the empirical results and the fifth section deals with the implications of the empirical key

strategies for the adoption of IaaS in Germany. The sixth section discusses the limitations of this study, and the final section outlines the conclusions and future work of the paper.

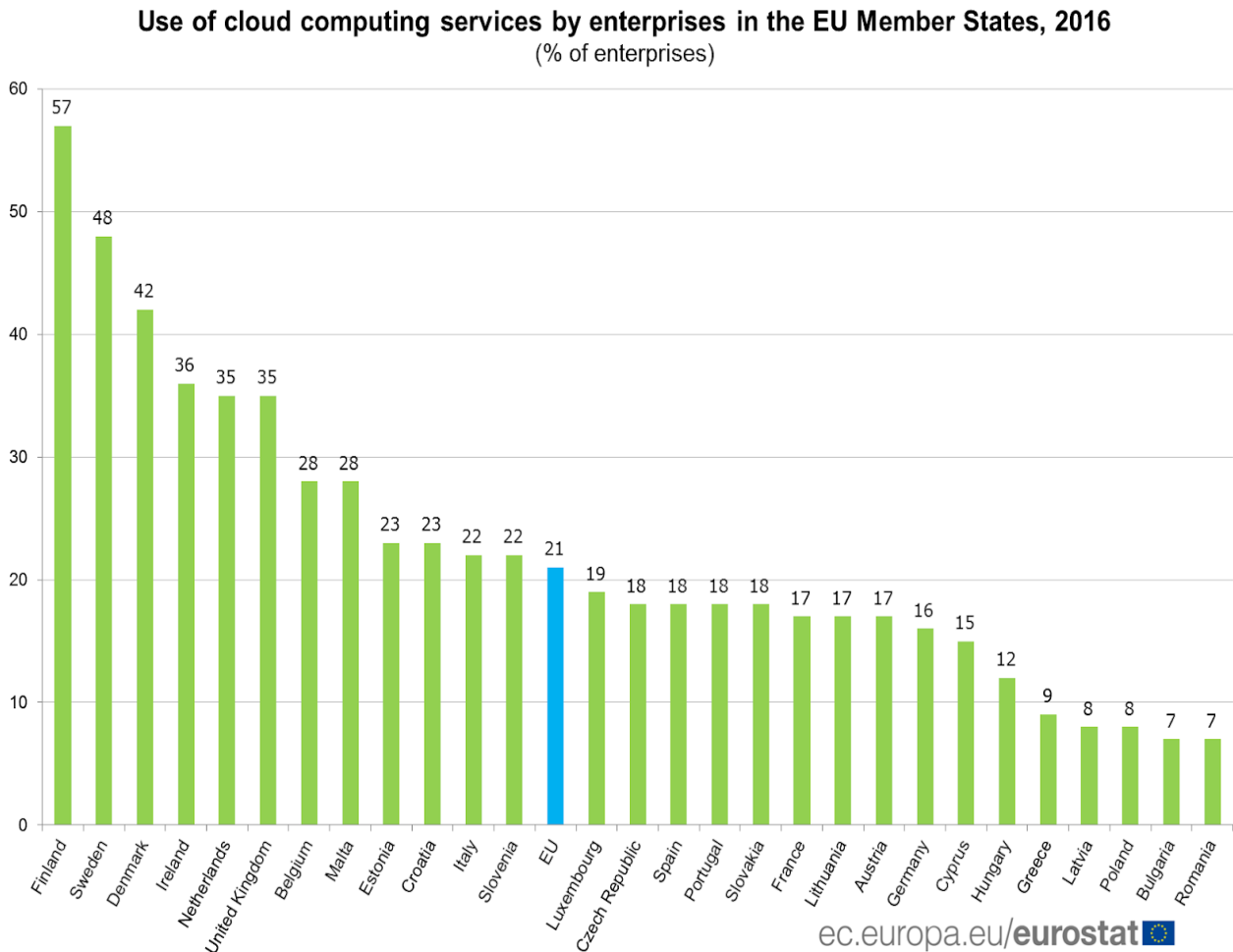


Fig. 1 There are significant differences between EU Member States. Over half of enterprises in Finland (57%) and over 40% in Sweden (48%) and Denmark (42%) use IaaS. On the opposite end of the scale, Germany has less than 20% of cloud usage.

3.0. Literature Review

In previous studies, various theories have been proposed to investigate factors that have increased technology acceptance. Some of the earlier models and theories are the Technology Acceptance Model (TAM) (Davis, 1986; Davis, 1989; Davis et al., 1989), Theory of Planned Behavior (TPB) (Ajzen, 1985; Ajzen, 1991), TAM 2 (Venkatesh & Davis, 2000), Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al., 2003).

The Theory of Reasoned Action (TRA) was proposed by Ajzen and Fishbein (1980) to explore the factors that influence the behaviour of individuals when using certain technologies. More specifically, TRA acknowledges behaviour and subjective norms as compulsory indicators of an individual's intention to use a specific technology. TRA implies that an individual's behavioural intention is a composite of his attitude to behaviour and perceived normative factors. This model refers to an individual's performance in terms of behaviour as attitude, in contrast to an overall performance of an individual (Fishbein & Ajzen, 1975). The subjective criterion is the individual's acceptance that a person who is valuable to him believes that he could engage in the implicit behaviour. In this way, TRA will not be suitable for our research because it anticipates behaviour when the conscious control of individuals is abused (Ajzen, 1991). In addition, it lacks the ability to identify convictions that are significant for a specific behaviour.

The Technology Acceptance Model (TAM) has been shown in the literature to be the most effective framework for verifying technology adoption plans. The fundamental aim of the model was to distinguish drivers that influence computer usage (Davis, 1989; Yang, 2005).

Similarly, Davis et al., (1989) took some basic factors that had been presented in previous studies as the main determinants of computer use and applied a psychologically based hypothesis (TAM) to model the relationships between these factors and to formulate hypotheses. Their study concluded that perceived usage (U), perceived ease of use (E), behaviour and usage influence the individual's expectation to use new technology. Perceived usefulness indicates the extent to which individuals accept that the use of a particular technology would improve their work performance. Perceived ease of use is the degree to which individuals believe that using a particular technology would be convenient (Davis, 1989). In summary, the intention to use a new technology is influenced by the perceived usefulness and perceived ease of use. Davis' research demonstrated that the relationship between usage and usefulness is more resilient than the relationship between use and usage.

Despite the robustness of TAM, several researchers have analysed the validity of TAM, TRA and TPB and their shortcomings (Ives & Olson, 1984; Venkatesh & Davis, 2000). Since the model was mainly developed in the United States, Straub et al (1997) and McCoy et al (2007) argued that TAM is not universally applicable and may not have the ability to predict the use of technology in different cultures. Venkatesh and Davis (2000) expanded TAM to TAM2 to overcome the above limitations by integrating social impact and cognitive tool based techniques as fundamental components of the adoption or use of information systems. Both U and E in TAM have also been criticised for tending to ignore the main factor that hinders the adoption of information systems (Luarn & Lin, 2005). Luarn &

Lin (2005) have proposed to integrate consumer trust elements (perceived credibility) and two asset elements (perceived self-viability and perceived financial cost) in TAM, as consumer trust indirectly influences the customer's intention to adopt new technologies based on E.

Stewart (2018) also proposed the integration of data security into TAM, as data security is the main determinant of consumer trust in the concept of using information systems. Here it becomes clear that a lack of data security awareness is a hindrance to the adoption of IaaS.

Tang et al (2004) and Wang et al (2003) examined the impact of data security and privacy concerns on the adoption of mobile banking using the TAM as a blueprint. Stewart (2018; 2017) highlighted data security and consumer trust as a significant determinant of technology adoption. As mentioned above, the two distinct TAM constructs were merged with the TRA model to form the internal-external element (value creation) construct in this paper. Therefore, in this study we examine the elements that affect IaaS by extending the TAM to include the elements of NFC factor (data security and consumer trust); we excluded the unified theory of acceptance and use of technology (UTAUT) (Venkatesh et al., 2003) due to its complexity (Venkatesh et al., 2003). In addition, UTAUT explores the construct of social impacts, which is not required in our current work. Further theories are summarized in Table.1.

Table 1. Different methodology and results used in IaaS adoption and the challenges.

Author + Research year	Method	Results
Sabi et al. (2016)	TAM and DOI	They proposed a model that assesses contextual, economic, and technological impacts in the observation and appropriation of IaaS at colleges in sub-Saharan Africa.
Salim Al (2016)	TOE and DOI	Technological, Organisational and Environmental factors were found and could be determinants of the adoption of IaaS services.
Rohani et al. (2015)	TTO, DOI, and TOE	This research identifies four contexts: Human characteristics, technological, organisational, and environmental which are essential elements for the adoption of Cloud.
Tashkandi et al. (2015)	TOE	Relative Advantage, Data Privacy, and Complexity are the most significant factors for cloud adoption.
Tiago Olivia et al. (2014)	TOE and DOI	Technology: Technology Readiness Organisation: Top Management Support , Firm size

		Environment: Competitive Pressure, Regulatory Support Innovation Characteristics: Relative advantage (cost saving, security concern), Complexity and Compatibility.
Yu-Ting Lee et al. (2013)	DEMATEL and TAM	As indicated by the outcomes, clear understanding and operating straightforwardness under the subject seeming convenience (PEOU) are increasingly basic; though improved value and efficiency under the topic saw helpfulness (PU) are progressively critical to apply.
Alharthi et al. (2012)	Integrated TAM mode (I-E factors	It is simple for foundations to embrace cloud in the event that they will have consumer trust beneficial to them through attitude, behavior and real use of IaaS.
Mohammed Khatib Juma, Aris Tjahyanto (2019)	ITOETAM	
H.Stewart (2018)	Intention to adopt Fintech	The challenges of FinTech acceptance in Germany.

3.0. Methodology

3.1. Research Framework and hypothesis

This study proposed an integrated theoretical framework for IaaS adoption in the financial sector based on TAM, TOE, and NFC (Davis, 1989; Oliveira et al. 2014; Stewart, 2017, 2018). The three theoretical frameworks have been used in studies on IT deployment and they complement each other. The TAM focuses on the characteristics of the technology and its acceptance (Davis, 1989; Davis et al., 1989), the TOE is a multi-perspective framework in which the environmental context influences the decision to introduce an innovation (Tornatzky & Fleischer, 1990), while the NFC focuses on information security and consumer trust. The NFC has been used to represent security, risk, and consumer trust in the acceptance of information technology. The framework focuses mainly on the characteristics of technology, humans, and data security (Stewart, 2017).

In this paper, the determinant of the acceptance of IaaS has been divided into five categories with associated variables: (i) NFC (data security, risk and consumer trust), (ii) technological factor (innovation

characteristics and opportunities), (iii) internal-external factor (value creation and management), (iv) organisational factor (size and vision) and (v) environmental factor (competitive pressure and government incentives). Furthermore, the TOE theory is a very useful analytical tool to explain the adoption of innovation by banks in Germany (Zhu et al., 2006b; Leinbach, 2008; Ifinedo, 2011), while NFC points to the need for security in cloud infrastructures (Stewart, 2017). This work is based on a quantitative study that identifies the challenges that banks in Germany face when moving to the cloud.

As discussed above, the proposed model consists of five constructs, each with its associated variables, and we expect that these constructs will influence banks' intentions to adopt IaaS services. The extended TAM, as shown in Figure 2, is referred to as "IaaS adoption". The decision to use the TAM as our research model to determine banks' intentions to adopt IaaS is attributed to its consistent ability to clarify the changes between intended behaviour and actual behaviour (King and He, 2016). In this paper, we empirically examine the components that influence the financial sector's expectations of IaaS adoption, such as data security, consumer trust, risk, value creation, opportunity, innovation, management, size, vision, competitive pressures and government incentives. Thus, data security, risk and consumer trust play a key role in this research, and we intend to look at them in context and in relation to other aspects, as we agree with the researchers who believe that these aspects should be considered together.

Table 2. Factors Impacting Banks in Germany

	Adoption Drivers	Constructs	Historical research
T	Technology	-Technology Opportunities (TO) -Innovation Characteristics (IC)	Studies (e.g., Kwon & Zmud, 1987) show that the successful adoption of IT depends on the importance of internal technology resource- infrastructure, technical skills, developers, and user time; therefore, firms with higher levels of technology competence show more likelihood to adopt new technology.
O	Organization:	-Firm's Size (FS) -Firm's Mission (FM)	Organization contexts for E-Commerce adoption measure principally descriptive factors. Besides the incumbent constructs (see Jeyaraj et al., 2006; Sabherwal et al., 2006; Tornatzky & Fleischer, 1990), this

			paper brought in individual difference factors, organization mission, facilitating conditions, and subjective norms.
E	Environment	-Competitive Pressure (CP) -Government Incentives (GI)	Organization’s propensity to innovate is shaped by environmental opportunities and threats. Strong correlation exists between a firm’s decision to use EC and such industry factors as peer influences, rate of technical change, market volatility and coercive influences perhaps from customers (Raymond & Blili, 1997). Tornatzky and Fleischer (1990) discussed the environment in terms of consumer readiness, competitive pressure, and trading partners’ readiness, while this paper adds perceived trust.
NFC	Nine Five Circle	-Data Security (DS) -Risk (R) -Consumer Trust (CT)	The NFC security framework indicates the necessities for the implementation of operational and information security enhancements. It also puts more emphasis on the measurement, the evaluation of organization information security management incidents (ISMI) performance and cloud outsourcing, as well as the enhancement of the interrelationship between technology and human factors. (Stewart, 2017; 2018).
IEF	Internal-External Factors	-Value Creation (VC) -Management (M)	(Agarwal & Prasad, 1999)

3.2. Research Theoretical Framework

The adoption of IaaS (IaaS) is a highly participatory decision and with it the need for a conscious search for the Bass Model to reduce the perceived technical, financial, consumer trust and security risks. Although this work does not aim to approximate the diffusion model developed by Frank Bass in 1960 to study the diffusion of different types of new products and services, it is a useful tool for predicting the initial adoption of an innovative product.

3.2.1. Research design and theoretical framework

In this study, we divide the methodology into two distinct segments. In the first segment, we develop a theoretical framework based on the literature and the information security hypothesis of this study. The second segment provides the empirical framework used to analyze the key factors driving the adoption of the IaaS-based approach among banks in Germany.

Table 3. Factors Impacting Banks in Germany

Factors	Description
NFC	Nine Five Circle
IEF	Internal-External Factor
TF	Technological Factor
OF	Organisational Factor
EF	Environmental Factor

We represent the internal and external components that influence the adoption of IaaS in our model by determining the internal-external factor (IEF). The two main TAM constructs: U and E, represent the internal elements that determine the IEF. According to TAM, the U is the individual's conviction that he or she can be more efficient when adapting to a new technology (Venkatesh et al., 2003), while the E is the conviction that a new technology is easy to use. In this respect, banks in Germany will opt for IaaS if it is useful and effortless. Thus, we have characterised our IEF as an arbitrary extension in the sense of U and the ability to use IaaS with less effort (E). In this way, the IEF captures the TAM variables U and E as precursors to the intention to use IaaS. This is similar to TRA, due to the aggregation of effort and usability, but unlike TAM, where the two constructs are treated differently (Pikkarainen et al., 2004). The external determinants of our IEF are determined by the efficiency of the secured connectivity and coverage, which provides banks with easy and consistent access when moving to the cloud (Venkatesh et al., 2003;). In this paper, various hypotheses for verification have been summarised in Table 4.

3.2.2. Hypothesis

The research deals with the challenges in implementing the IaaS adoption model to the banks and in Germany. The study was designed to hypothesize the following proposition.

Table 4. Research Hypotheses in this study

	Hypotheses	Source
H _a	Banks in Germany's intention to adopt IaaS are not always influenced by the organisational factor.	(Grazioli and Jarvenpaa, 2000) (Datta, 2011)
H _b	Consumer trust does not always influence organisations' intention to adopt cloud platforms (IaaS).	(Whitman and Mattord, 2009) (Yao et al., 2003)
H _c	The willingness of banks in Germany to trust IaaS is not influenced by data security.	(Amoroso and Hunsinger, 2009) (Joseph et al., 2012) (Stewart, 2018)
H _d	Data security does not influence banks in Germany's intention to adopt IaaS.	(Lee and Chung, 2009) (Stewart, 2018)
H _e	Banks in Germany' intention to adopt IaaS is not influenced by the technological factor.	(Lanford, 2006) (Laberge and Caird, 2000)
H _f	Technological factors do not influence the willingness of banks in Germany to adopt IaaS.	(Stewart, 2018)
H _g	Environmental factor is not a vital determinant of consumer trust in banks' intention to adopt IaaS	(Pikkarainen et al., 2004) (Howcroft et al., 2002)

In addition, IaaS providers with rigid security measures should use advertising for their services (Kritzinger and vom Solms, 2010; Parker et al., 2015). In this sense, the present study proposes the following theories:

Table 4.A. Research Hypotheses

H _h	Organisational factors do not influence banks in Germany's intention to adopt IaaS.
H _i	Organisational factors are not influenced by NFC factors.
H _j	Organisational factors are not influenced by the environmental factors.
H _k	Organisational factors are not influenced by the technological factors.
H _l	Environmental factors do not influence consumer trust in German banks' intention to adopt IaaS.

In the above analysis, the relationships between the hypothetical constructs and the variables are analysed. The hypothetical structure developed in our work is intended to show that the organisational factor, technological factor, internal-external factor, environmental factor and the NFC factor are the possible precursors for the adoption of IaaS by banks in Germany, which refines the hypotheses for the adoption of IaaS in Germany. Figure 2 integrates the constructs of TAM into the TOE and the NFC and adds individual different factors (IDF), thereby facilitating the conditions (FC), the organisational mission (OM), the perceived trust (PT) and the perceived quality of service (PSQ). The NFC elements that influence the introduction of IaaS are represented in our model by the determinant data security (DS), consumer trust (CT) and risk (R). The integration of the constructs of TAM, TPB and TOE into the model is in a sense social and behavioural constructivism to promote the banking sector's intention to adopt IaaS. The postulate of this model is similar to actor network theory (ANT) in that it emphasises the dynamic and mutual interaction of technical and social systems.

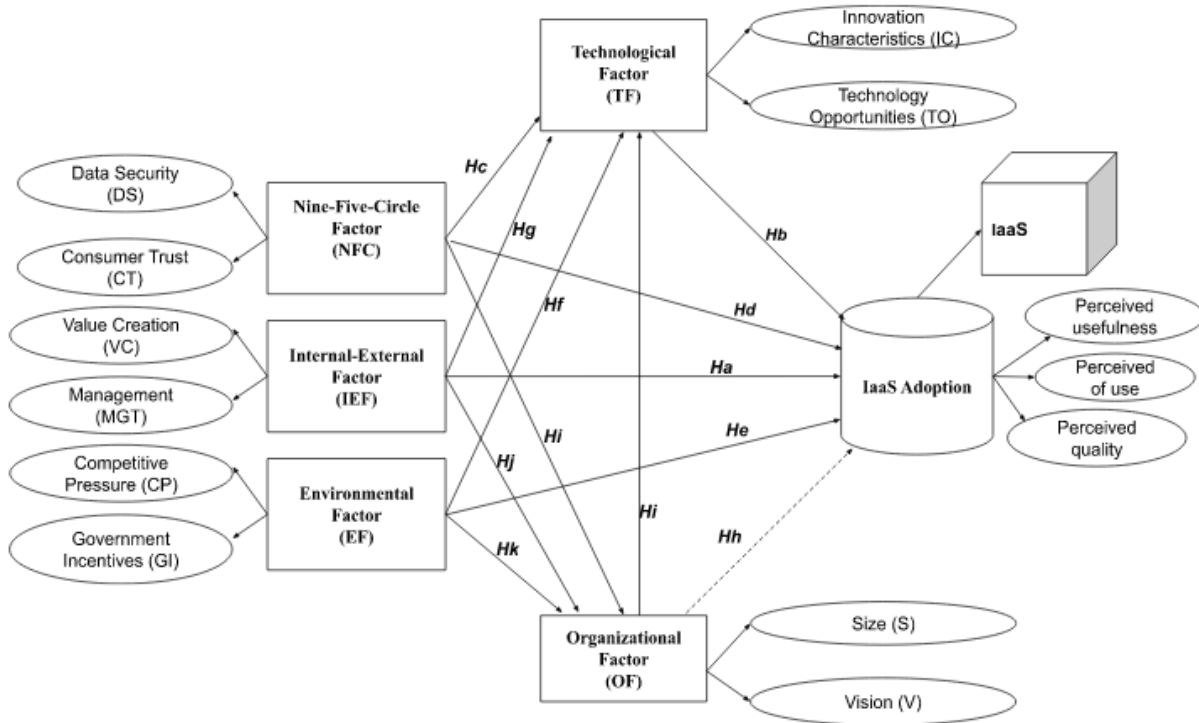


Figure 2: Proposed Research Model - Banks in Germany IaaS Adoption

Under the guidance of the TAM and our verifiable hypothesis, we had the opportunity to identify both the internal and external factors that can determine the adoption of IaaS. At this stage, however, we

cannot relate our hypothesis derived from our verifiable hypothesis to our research questions, as the after-effects of our hypothesis and the critical balance of our five factors are very delicate. At this stage, we can only expect that these five factors will be able to convince and influence the Bank's intention to adopt IaaS.

3.3. Empirical Method

3.3.1. Sampling and Data Collection

The goal for this data collection was to evaluate banks' perceptions of data security concerns and consumer trust in the intention to adopt IaaS (Ashley and Boyd, 2006). The study used a survey as a method of data collection, questionnaires sent directly to respondents via e-mail and telephone message. As a rule of thumb, our respondents consist of regional, large commercial banks established under the German Banking Act. Each of the banks is affiliated with National Planning and Economic Development. All of the banks provide commercial banking services. The vision of each of these banks is to become an innovative and dynamic bank with a strong commitment to achieving positive and sustainable outcomes for all stakeholders and customers. A sample size of 208 respondents comprises the employees selected to respond to the questionnaire. The questionnaire consists of two sections, i.e. (A and B), with section A consisting of demographic questions and section B consisting of a five-level Likert scale, ranging from 1-strike positive to 5-strike negative. In order to align our questions with our hypotheses, the 40 questions were posed to the respondents to assess their quality. This approach enabled us to use figures to clarify questions on the basis of research by Lundahl and Skärvad (1992) and to summarize the results for the populace, as conducted by Burns and Grove (2001). The original sample of questionnaires sent out was 298, of which 90 questionnaires were rejected as unsatisfactory or unnecessary. The remaining 208 questionnaires were considered an acceptable sample size as they represented a response rate of 53.8%. We used a stratified sample design to select our sample participants. Table 5 illustrates the relationship between the questions, variables, and hypotheses.

Table 5. Survey Questions, Hypotheses, Variables

	Hypotheses	Questions
Demographic	-	Q1 - Q4
Nine-Five-Circle Factor	H _c , H _d	Q4 - Q16
Internal-External Factor	H _b	Q17 - Q22

Technological Factor	H _f , H _h	Q23 - Q29
Organisational Factor	H _a , H _b , H _i	Q30 - Q35
Environmental Factor	H _k - H _n	Q36 - Q40

The SPSS AMOS is used to analyze the data, which includes validity tests, descriptive statistical analysis, confirmatory analysis, exploratory factor analysis (EFA) and univariate analysis. This paper attempts a three-step approach.

In the first stage we analyse the data using EFA and a canonical correlation matrix for data decrements. A preparatory workshop for a pilot study provided the participants with the questions and ensured that all participants understood the motives for the research. Here 90 samples were used for the pilot study. We applied the technique of principal axis factorisation in a Promax rotation to limit the items of each loaded latent factor. Each question was decoded using different techniques to ensure that all participants understood each question in the same way. We obtained a set of five different eigenvalue factors that validated the five factors in the literature review and further tested their reliability using Cronbach's Alpha (Cuieford, 1965). Cronbach's alpha is used to measure the reliability of the different Likert questions in a questionnaire that forms a scale (Allen and Yen, 2002; Bland and Altman, 1997; Cuieford, 1965). According to Cuieford, 0.7 of Cronbach's alpha is high enough in an exploratory research test and therefore researchers should aim for values between 0.35 and 0.7 and reject all values below 0.35.

The second stage of the approach involves estimating the measurement model using Confirmatory Factor Analysis (CFA). In this stage, the discriminant validity, reliability and convergence of our factors are transformed into a data set of 198 samples.

Finally, we use a structural equation model (PLS-SEM) derived from all models that were used to test our hypothesis. The structural equation framework of SPSS AMOS is used in our work. In this study, X_i stands for the latent variable that measures the banks' intention to adopt IaaS from the total number of respondents. The correlation that exists between X_i and an explanatory set of variables is given by r_i .

$$X_i = r'_i \beta + \epsilon \tag{i}$$

The determinants that influence IaaS adoption are represented by the vector:

$$r' = [\text{OG, TF, NFC, EF, IEF}]'$$

The explanatory variables in this work are exogenous variables and represent latent variables (V) which are measured by two or more perceived marker variables (Y). This then gives us the equation:

$$Y_i = L_v V + \epsilon_v \quad (ii)$$

Where:

Y_i =Vector of the marker

V =Exogenous factor

ϵ_v =Measurement error hl

L_v =Loading

Figure 2 shows a model to predict the perceived intention of banks in Germany to migrate to a cloud environment (IaaS) based on the constructs; (i) organisation factor, (ii) technology factor, (iii) environmental factor, (iv) NFC factor, and (v) internal-external factor using AMOS and the Statistical Package for Social Science (SPSS). A structural equation model (PLS-SEM) was applied to evaluate hypothetical relationships between our constructs and to validate the scientific behavioural approach of our study as well as to estimate multi-correlations. The PLS-SEM system is capable of generating large mean square errors in path coefficient estimation, and since arrows are single-headed without exception, it is not capable of modeling a 2-way correlation. All this has helped us to construct all our hypotheses, which allowed us to present them with latent variables (Sadeghi and Hanzaee, 2010). In addition, the PLS-SEM is a useful statistical tool for the specific situation, especially in situations where an accurate model specification cannot be guaranteed or the sample size is small and where predictive accuracy is of utmost importance and the application has a specific theory.

3.3.2. Applying SEM (Measuring of structural and measurement model)

As a rule, we followed six basic steps. The first step, also known as model specification, was to define the hypothetical relationships between the manifest variables (MV) and our latent variable (LV). We derived our relationships based on the current literature and existing theories. As shown in Figure 2, we represented our latent variable by "IaaS adoption" and by manifest variables (TF, OF, EF, IEF and NFC) represented by squares. The arrows illustrate the hypothetical relationships as shown in Figure 2. Our next step was to determine our model (also known as model identification) to validate whether the model is suitable in relation to the degree of freedom to be calculated. To determine the degree of freedom of the model, the number of parameters to be evaluated is subtracted from the number of known components. As Gefen et al. (2000) state, a model is over-identified if the degree of freedom is

greater than zero. However, for the analysis of our model it was essential to ensure that it was over-identified.

Step 2 consisted of data collection. During this phase, previous studies were followed, such as the correct sample size. A number of researchers have recommended limiting the threshold for sample size to 10 and, in the case of complex constructs, multiplying the number by the number of items (Gefen et al., 2000). Kline (1998), suggested 10 to 20 participants for hypothetical relationships between two variables, while Weston et al. (2006) proposed a standard sample size of 200 for the PLS-SEM.

Multicollinearity refers to the fact that there is a solid relationship between measured variables ($r > 0.85$). In this study we considered eliminating all items that could cause multicollinearity. Since the focus of our work was only on banks in Germany, we tried to adhere to the cases applicable to Germany and to characterise cases that were not significant for Germany as outliers. According to Field (2005) outliers allude to cases that are considered abnormal, similar to the main pattern of the data. In this work we eliminated both outliers and missing data before applying PLS-SEM to avoid any bias.

The model was then estimated by determining the value of the obscure parameters and the error relationship to the estimated value. Prior to the structural model estimates, we tested the measurement model using confirmatory factor analysis (Anderson and Gerbing, 1988; Weston et al., 2006).

The next phase was the model evaluation, which was also called model fit and interpretation. Here the fit was evaluated on the basis of the following conditions: (i) the strength and significance of our hypothetical relationships, (ii) the variation clarified by our latent variables and the observed origin, and (iii) the consistency of our model with our observed data.

The SPSS, AMOS and the Cetbix RM were used for data analysis in this study. SPSS enabled us to perform descriptive analysis, exploratory factor analysis, normality test, reliability test, outliers' detection and missing data detection. The Cetbix RM was used for our questionnaire to determine our constructs. The data was stored on Cetbix RM, which was later transferred from SPSS to AMOS. We performed both our CFA and structural model analysis with AMOS. In general, the PLS-SEM is a useful statistical tool for the specific situation, especially in situations where an exact model specification cannot be guaranteed or the sample size is small and where prediction accuracy is of utmost importance and the application has a certain theory.

4.0. Findings and discussion

This study has been undertaken to identify the main factors influencing and driving the adoption of IaaS. Our exploratory factors are the technological factor (TF), the organisational factor (OF), the environmental factor (EF), the internal-external factor (IEF) and the Nine-Five-Circle factor (NFC). The CFA was used to test the discriminatory validity, convergence and reliability of each variable. Our composite reliability value was set at 0.7 or higher and the outer load was set at 0.7. The convergent validity (AVE) value was set to 0.5 or higher [16], and our Cronbach alpha was set at a rate of 0.7 or higher (Cuietford, 1965; Hair et al., 1998). Figure 1 shows the number of uses of cloud computing in Germany. It is fascinating to observe that 99% of the respondents are familiar with IaaS, but only 1% have recognised the benefits of IaaS. It is also clearly discouraging to see that only 3 out of 208 respondents use IaaS services, which is less than 1% of the respondents. The CFA was used to assess the discriminatory validity, convergence and reliability of each variable, as shown in Tables 6 and 7.

We tested our hypotheses through several surveys to determine the intentions of banks to adopt IaaS. According to the guidelines of Cuietford (1965) and Hair et al (1998), Cronbach's alpha rate was above 0.7, although Hair et al. also recommended a rate of 0.6 in an exploratory study. As shown in Table 7, NFC loading factor is 0.97 and with Cronbach's alpha rate of 0.57, which is below the two standards recommended by Cuietford (1965) and Hair et al (1998). The normal loading factor is characterised as a statistical strategy that shows relationships among items and factors (Tucker and MacCallum, 1993).

The normal loading factor for the technology construct factor (TF) is 0.66, with a Cronbach alpha of 0.79.

The normal loading factor for the internal and external factor (IEF) is 0.59, with a Cronbach alpha of 0.93.

The normal loading factor for the environmental factor (EF) is 0.98 with a Cronbach Alpha of 0.91.

All our Cronbach Alpha values are higher than 0.7 for all our designs, except NFC. In short, the confirmatory factor analysis has revealed the importance of all designs tested in the EFA. Consequently, we identified the factors that influence the acceptance of IaaS as OF, TF, IEF and EF and correlated them with NFC. The convergent validity of our constructs was examined by determining their average variances (AVE) (Farrell, 2009). Our AVE exceeded 0.05 for our construct measurement as recommended by (Cortina, 1993; Costello and Osborne, 2005).

There were no significant deviations in the results with regard to standards and exceptions. The model is identified by the SEM. Usually, in the early phase of the SEM the recommended suggestions of the related models such as, Tucker-Lewis Index (TLI), Relative Chi-Square (CMIN), Normalized Fit Index (NFI), Comparative Fit Index (CFI) sparse Comparative Fit Index (PCFI) and Mean Square of Approximation (RMSEA) are identified. As shown in Figure 3, the SEM model fits best to our data.

Table 6. Banks and their readiness in cloud platform survey questions, Hypotheses and Variables

	Cloud Infrastructure User		Cloud Infrastructure Awareness	
	Frequency	%	Frequency	%
Yes	3	1	208	100
No	205	99	0	0
Sum	208	100	208	100

Table 7. Confirmatory Factor Analysis of Latent Reliability and Convergence Validity

Constructs	Cloud Infrastructure User		Cloud Infrastructure Awareness	
	Items	Normal Loading Factory	Cronbach's Alpha	Average Variance Extracted
Nine-Five-Circle (NFC)	NFC	0.97	0.57	0.67
Internal-External Factors (IEF)	IEF	0.59	0.93	0.48
Technological Factor (TF)	TF	0.66	0.79	0.53
Environmental Factors (EF)	EF	0.98	0.91	0.92
Organisational Factor (OF)	OF	0.73	0.87	0.47

As mentioned above, our explanatory variables are exogenous and represent latent variables (V), which we measured using two or more perceived marker variables (Y) and grouped into items, as shown in Table 8.

Table 8. Confirmatory Factor Analysis of Discriminating Validity

OF	NFC	TF	IEF	EF	
0.477					OG

0.20	0.669				NFC
0.057	0.351	0.032			TF
-0.112	0.27	0.097	0.31		IEF
0.157	0.03	0.021	0.087	0.781	EF

NFC [Nine-Five-Circle] IEF [Internal-External Factors] TF [Technological Factor] [EF]Environmental Factors [OF] Organisational Factor

Based on the Fornell-larcker criterion, the discriminant validity measure suggested as the square root of AVE in each construct could be used to set up discriminant validity if the value is larger than the other correlation diagonally. For example, from table 7 the constructs AVE of NFC, IEF, TF, EF and OF found to have the square root of 0.67, 0.48, 0.53, 0.92, and 0.47 respectively, these values are larger than the correlation value of their respective columns. Thus, the result indicates that the discriminant validity is well established as displayed in Table 8. Our parsimonious indices indicate our model fits (PCFI = .84). The data in Table 9 show that all parameters determined are essential in our hypothesis. Although our CMIN is not within the required limit of 3.0 as suggested by Chau (1997), it is still reasonable as it is between 0.05 and 0.08, which is considered a suitable model fit as shown in the work of MacCallum et al. (1996). Like Steenkamp and Van Trijp (1991), our comparative fit indices demonstrate model fits as follows:

(CFI = 0.97), (NFI = 0 .92) and (TLI = 0 .93).

As a result, the observations lead to the conclusion that our model fits well with the sample data of the work.

Table 9. Final Confirmatory Factor Analysis Model for our Model Fit

Fit Measures	Values Proposed	Values Observed
CMIN (χ^2/df)	≤ 3.0	1.79
Normed Fit Index	$\geq .90$	0.92
Parsimony adjusted to CFI	-	0.81
Tucker-Lewis Index	$\geq .90$	0.93
Comparative Fit Index	$\geq .90$	0.97
Root mean square error of approximation	$\leq .08$	0.05

After having analyzed our model fit, we conclude from our empirical results that the IEF has significant potential to influence the decision to adopt IaaS as well as EF. In this respect, the results indicate a 1% degree of influence, and the empirical results suggest that banks in Germany are more likely to adopt IaaS if they see its value creation. The results in this paper confirm that the influence of organisational factors has no direct or indirect impact on the uptake of IaaS.

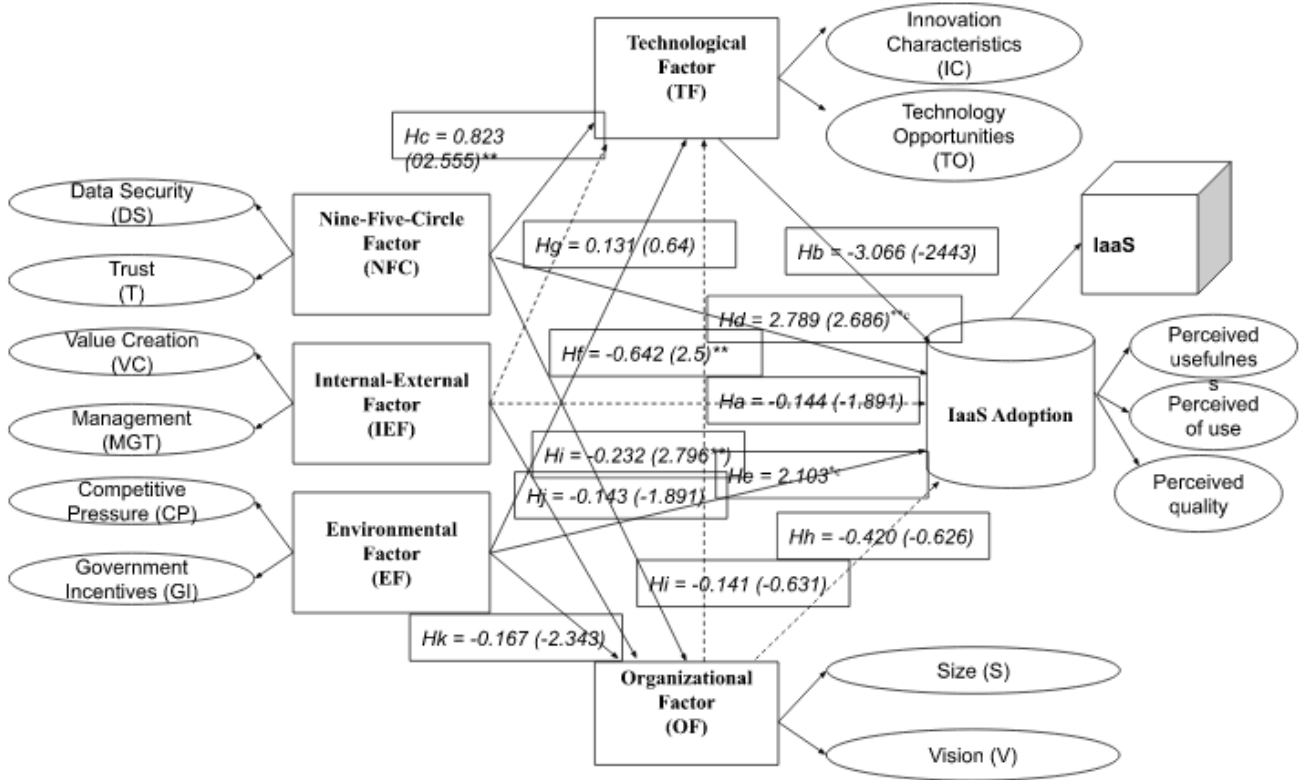


Fig. 3 Proposed Research Model Fit- IaaS Adoption in Germany

We have based our standardized regression weight on the y-value, where $^{**}y < 0.01$,

$^*y < 0.05$.x-path, which was set to 1.0 for model identification.

4.1. Univariate Analysis

Given the results obtained in this study, as shown in Table 10, there is sufficient evidence to support the rejection of Hb , Hc and Hd . This indicates that data security does influence consumer trust due to the close correlation between quality and consumer trust. With regard to competitive pressure, IaaS

vendors should emphasize security, distinctiveness and privacy as clear variables of consumer trust models. As suggested by Donahue et al (1999), convenience is seen as a clear factor for seamless business, however Stewart (2020) alluded that convenience alone does not influence the acceptance of technology. IaaS vendors will gain more consumer trust from FinTech incubators than from the traditional banks due to the attractiveness and cost factor of IaaS. Berger and Sasse (2001) argued that various variables can be explained as consumer trust, and Stewart (2020) argued that most organisations will ultimately address cyber security risks effectively before migrating to the cloud.

Furthermore, Hc is rejected because data security with a trust level of about 99% strongly influences banks consumer trust. Furthermore, the results Hg, Hi, Hj, and Hk are not rejected. These indicate that NFC factors (data security, consumer trust & risk) and environmental factors influence organisational factors. The results reject Hb, Hc, Hd, He and Hf with a confidence level of 99%. Collectively, it implies that there is a hierarchy of significant variables where NFC factor (data security, consumer trust), environmental factor (government incentives), and technological factor (innovation characteristics, technology opportunities) are the main elements of banks' intent to adopt IaaS. However, the difference in the mean value is small, especially between user environmental factors and NFC factors. Therefore, we can confidently conclude that all three factors have an impact on IaaS adoption by the banks in Germany.

Hh is insufficient to draw the conclusion that organisational factors influence the intention to adopt IaaS. Hl is not rejected.

This analysis allows us to answer our research questions regarding the main obstacles to IaaS adoption and the factors that banks prioritize in the context of IaaS.

Table 10 Univariate Analysis Results

	Hypothesis	Univariate Analysis
--	------------	---------------------

<i>Hb</i>	Consumer trust does not always influence organisations' intention to adopt cloud platforms (IaaS).	<i>Rejected</i>
<i>Hc</i>	The willingness of banks in Germany to trust IaaS is not influenced by data security.	<i>Rejected</i>
<i>Hd</i>	Data security does not influence banks in Germany's intention to adopt IaaS.	<i>Rejected</i>
<i>He</i>	Banks in Germany' intention to adopt IaaS is not influenced by the technological factor.	<i>Rejected</i>
<i>Hf</i>	Government incentives do not influence the willingness of banks in Germany to adopt IaaS.	<i>Rejected</i>

5.0. Limitations

This research focuses on studies that evaluate the challenges of IaaS acceptance in Germany. In this study there are some limitations that are disclosed to illustrate the exploratory approach. First, our study focuses on IaaS acceptance among banks in Germany and not throughout Europe. The selected period of study is based on the years 2019-2020. Future analysts can support the research of this topic by changing the determinants in the UTAUT model. Since we have adopted the cluster sampling technique, the reported results are not 100% generalized for all financial institutions in Germany. Therefore, the researchers strongly recommend that additional research be conducted in this area of study. IaaS is still a new phenomenon and less has been studied on the challenges faced by the banks in Germany. In our next study, we will include a complete cross-over, a basic sampling strategy for all financial institutions in Europe. The researchers speculate that the current outcome of this research would be somewhat different in other parts of the world. Therefore, our results are only generalized for the country of Germany and not for other geographical areas. Nevertheless, the demographic and social effects were neglected because the corresponding items disregarded the reliability of the model. Therefore, our results are only generalized for the country of Germany and not other geographical areas. We also assume that some of the questions were neglected due to the respondents' reaction. For example, those who were uncertain about the subject matter of the survey. In spite of this, demographics and social impact were neglected since their corresponding items disregarded the instrument dependability. All the factors neglected were not quantifiable on IaaS adoption.

6.0. Conclusion

Based on this result, the study concludes that H_b, H_c and H_d were rejected while four hypotheses (H_a, H_e, H_f and H_g) were accepted. The four hypotheses were accepted and proved to be the strong correlation between the laaS adoption model and the factors studied (Figures 2 and 3). The observation indicates that the NFC factors (data security, consumer trust and risk), technological factors (opportunities and innovation characteristics) and environmental factor (government incentives) and internal-external factors (management and value-added), have proven to be a statistically significant challenge in implementing the laaS adoption model for banks in Germany. The empirical study was conducted with the TAM, the TOE and the NFC. An important goal of this study was to go beyond the TAM standard so that we could address all the constraints associated with the TAM by integrating it as a key component in the deployment and use of laaS.

It was also crucial for us to go beyond the TAM standard, as TAM only focuses on perceived benefits and perceived usability. The perceived benefits and perceived usability ignore the limitations that stand in the way of adopting laaS. The result, backed up by statistical analysis, confirms that TF as well as IEF and NFC form a solid foundation for the adoption of laaS. Most importantly, these three factors have a significant impact on the adoption of laaS, while NFC has a significant impact on TF. Based on our results, we can answer the first and second questions positively, while emphasizing that the main obstacles to laaS innovation are data security, consumer trust and insufficient innovation characteristics. Therefore, it is important to address issues of data security and consumer trust in laaS. Awareness of how data is collected and used remains an important issue in the context of technology in Germany and answers our third research question. The current analysis demonstrates that the perceived benefits in terms of fraud protection and privacy are an immediate effect on the intention to adopt laaS.

Our last research question relates to the extent to which data security and consumer trust are important in the context of laaS. Here we have shown that consumer trust reduces risk perception when adopting laaS, i.e., there is a belief that banks can introduce laaS if they believe that their data is secured and guaranteed. This increases banks' consumer trust and affects their desire to adopt laaS services. The more banks are educated about the security of their data, the more their consumer trust in laaS will increase. It is therefore important that laaS providers understand the banks' attitude to data and increase data transparency and security to the awareness of the banks about how data is used and stored securely

For IaaS to achieve the maximum capacity guaranteed by the innovation, it must generally offer strong data security. This study, based on the given difficulties, prescribes the best measure to solve these difficulties by presenting the "IaaS" model with the TAM, TOE and the NFC framework.

The researchers propose the integration of data security and consumer trust in TAM in all technology adoption, as data security is the most important determinant of consumer trust in the concept of using information systems. It is clear here that a lack of data security awareness is a barrier to the adoption of IaaS in Germany.

Reference

- Al-shqeerat K, and KHA. Al-shqeerat. (2017), "Cloud Computing Security Challenges in Higher Educational Institutions -A Survey Cloud Computing Security Challenges in Higher Educational Institutions - A Survey 2017." doi:10.5120/ijca2017913217.
- Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2012), "A survey on security issues and solutions at different layers of Cloud computing", *The Journal of Supercomputing*, Vol. 63, Issue 2, pp. 561–592.
- Coppolino, L., D'Antonio, S., Mazzeo, G., & Romano, L. (2016), "Cloud security: Emerging threats and current solutions", *Computers & Electrical Engineering*.
<https://doi.org/10.1016/j.compeleceng.2016.03.004>
- Ramachandran, M. (2015), "Software security requirements management as an emerging cloud computing service", *International Journal of Information Management*, Vol. 36, Issue 4, pp. 580-590
- Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010), "A view of Cloud computing", *Commun. ACM*, 53(4):50–58.
- Suthaharan, S., & Panchagnula, T. (2012, March), "Relevance feature selection with data cleaning for intrusion detection system", In *2012 Proceedings of IEEE Southeastcon* (pp. 1-6). IEEE.
- Sari, A. (2015), "A review of anomaly detection systems in cloud networks and survey of cloud security measures in cloud storage applications", *Journal of Information Security*, 6(02), 142.
- Djemame .K. (2016), "A Risk Assessment Framework for Cloud Computing".
- Nada. M, Youssef. B, Brahim. B and Boubker. R. (2017), "Survey: Risk Assessment Models for Cloud Computing: Evaluation Criteria," in *2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech)* 1: 3–7.
- Rot. A. (2017), "Selected Issues of IT Risk Management in the Cloud Computing Model. Theory and Practice," no. *Imcic*. pp. 89–94.

- Shareeful. I, Fenz. S, Weippl. E, and Mouratidis. H. (2017), "A Risk Management Framework for Cloud Migration Decision Support".
- Wang. R (2017), "Research on Data Security Technology Based on Cloud Storage," *Procedia Eng.* 174: 1340–1355.
- Gholami. A, and Laure. E. (2015), "Security and Privacy of Sensitive Data in Cloud Computing" : A Survey of Recent Developments. pp. 131–150.
- Chou. T. (2013), "Security Threats on Cloud Computing." *International Journal of Computer Science & Information Technology (IJCSIT)* 5(3): 79–88.
- Kozlov. A. D, and Noga. N. L. (2018), "Risk Management for Information Security of Corporate Information Systems Using Cloud Technology," *Elev. Int. Conf. Management large-scale Syst. Dev. (MLSD)*. pp. 1–5.
- Esposito. C. and Castiglione. A. (2017), "Challenges of Connecting Edge and Cloud Computing": A Security and Forensic Perspective. pp. 13–17.
- Armbrust. M, Joseph A. D., Katz. R. H., and Patterson. D. A. (2009), "Above the Clouds: A Berkeley View of Cloud Computing".
- Mostajeran. E, Nizam. M, Mydin. M, Khalid. M. F, Ismail. B. I, and Kandan. R. (2017), "Quantitative Risk Assessment of Container Based Cloud Platform".
- Belbergui. C. (2017), "Cloud Computing" : Overview and Risk Identification Based on Classification by Type.
- Lee. K. (2012) "Security Threats in Cloud Computing Environments." *International Journal of Security and its Applications* 6 (4): 25–32.
- Davis, F., Richard, P.B. and Paul, R.W. (1989), "User acceptance of computer technology: a comparison of two theoretical models", *Management Science* 35(8), pp. 982-1003.
- Davis. F. (1989), "Perceived usefulness, perceived ease of use, and user acceptance of information technology", *Management Information Systems Quarterly*, 13(3), pp. 319-340.
- Oliveira,T. and Thomas,M. and Espadanal, M. (2014), "Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors". *Journal of Information & Management*, 51, pp.497–510
- Ifinedo. P. (2011a), "An empirical analysis of factors influencing Internet/E-Business technologies adoption by SMEs in Canada", *International Journal of Information Technology & Decision*.
- Tornatzky, L.G. and Fleischer, M. (1990), "The Processes of Technological Innovation", Lexington Books, Lexington, MA.
- Leinbach, T. R.(2008),"Global E-Commerce: Impacts of National Environment and Policy", edited by Kenneth L. Kraemer, Jason Dedrick, Nigel P. Melville, and Kevin Zhu. Cambridge: Cambridge University Press. *The Information Society*, 24, pp.123-125.

- Zhu, K., Kraemer, K. L., & Xu, S. (2006), "The process of innovation assimilation by firms in different countries: A technology diffusion perspective". *Management Science*, 52, pp.1557–1576.
- Dillon, A. & Morris, M. G. (1996), "User acceptance of information technology: Theories and models". *Annual Review of Information Science and Technology*, 31, 3-32.
- Tang, T. I., Lin, H. H., Wang, Y. S., & Wang, Y. M. (2004), "Toward an understanding of the behavioural intention to use mobile banking services", *PACIS 2004 Proceedings*, 131, <http://aisel.aisnet.org/pacis2004/131>
- Sun, H. (2003), "An integrative analysis of TAM: Toward a deeper understanding of technology acceptance model", In: *Proceedings of the 9th American Conference on Information Systems*, p. 2255.
- King, W. R. & He, J. (2016), "A meta-analysis of the technology acceptance model". *Information & Management*, 43, 740-755.
- Kwon, T. H. and Zmud, R. W. (1987), *Unifying the Fragmented Models of Information Systems Implementation*. In: Boland, R J and Hirschheim R A (eds): *Critical Issues in Information Systems Research*. Wiley & Sons (227-251).
- Venkatesh, V. & Davis, F. D. (2000), "A theoretical extension of the technology acceptance model: Four longitudinal field studies". *Management Science*, 45, 186-204.
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003), "User acceptance of information technology: Toward a unified view". *MIS Quarterly*, 27, 186-204.
- Ashley, P. & Boyd, P. (2006), "Quantitative and qualitative approaches to research in environmental management". *Australasian Journal of Environmental Management*, 13, 70- 78.
- Lundahl, U. & Skärvad, P. H. (1992), "Utredningsmetodik för samhällsvetare och ekonomer", 2nd edition. Sweden: Student literatur.
- Gefen, D., Straub, D. W. & Boudreau, M.-C. (2000), "Structural equation modeling and regression: Guidelines for research practice". *Communications of AIS*, 4,7, 1-80.
- Anderson, J. C. & Gerbing, D. C. (1988), "Structural equation modeling in practice: A review and recommended two-step approach". *Psychological Bulletin*, 103, 411- 423.
- Weston, R., Paul, A. & Gore, J. (2006), "A brief guide to structural equation modeling". *The Counseling Psychologist*, 34, 5, 719-751.
- Kline, R. B. (1998), "Principles and practice of structural equation modeling". New York, NY: Guilford.
- Field, A. (2005), "Discovering statistics using SPSS", London, UK: Sage Publications.
- Bass, F. M. (1969), "Bass Model" *Management Sci* 15 (5).
- Burns, N. & Grove, S. K. (2001), "The practice of nursing research: Conduct, critique, and utilization". Philadelphia, PA: Saunders.

- Cuieford, J. P. (1965), "Fundamental statistics in psychology and education", 4th ed. New York, NY: McGraw-Hill.
- Sadeghi, T. & Hanzae, H. K. (2010), "Customer satisfaction factors (CSFs) with online banking services in an Islamic country: I.R. Iran". *Journal of Islamic Marketing*, 1, 3, 249-267.
- Allen, M. J. & Yen, W. M. (2002), "Introduction to measurement theory". Long Grove, IL: Waveland Press.
- H.Stewart (2020), "INFORMATION TECHNOLOGY AND CYBER SECURITY UNPLUGGED: The interrelationship between Human, Technology and Cyber Crime Today", 1th ed. New York, NY: ROHHAT.
- Bland, J. M. & Altman, D. G. (1997), "Statistics notes: Cronbach's alpha". *BMJ*, 314 (7080):doi: <http://dx.doi.org/10.1136/bmj.314.7080.572>.
- Chau, P. Y .K. (1997), "Reexamining a model for evaluating information center success using a structural equation modeling approach", *Decision Sciences*, 28(2), 309-334.
doi:10.1111/j.1540-5915.1997.tb01313.x.
- MacCallum, R.C., Browne, M.W., Sugawara, H.M. (1996), "Power Analysis and Determination of Sample Size for Covariance Structure Modeling ", *Psychological Methods*, 1:130-49.
- Steenkamp, J. E. M. & Van Trijp, H. C. M. (1991), "The use of LISREL in validating marketing constructs". *International Journal of Research in Marketing*, 8, 283-299.
- Tucker, L. & MacCallum R. (1993), "Exploratory factor analysis: A book manuscript, available at: <http://www.unc.edu/~rcm/book/factornew.htm> (Accessed 3 August 2019).
- Farrell, A. M. (2009), "Insufficient discriminant validity: A comment on Bove, Pervan, Beatty and Shiu". *Journal of Business Research*, 63, 324-327.
- Cortina, J. M. (1993), "What is Coefficient Alpha? An Examination of Theory and Applications". *Journal of Applied Psychology*, 78, 1, 98-107.
- Costello, A. B. & Osborne, J. W. (2005), "Best practices in exploratory factor analysis: Four recommendations for getting the most from your analysis". *Practical Assessment, Research and Evaluation*, 10, 7.
- Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998), "Multivariate analysis", 5th ed., Englewood Cliffs, NJ: Prentice Hall International.
- Wang, Y. S., Wang, Y. M., Lin, H. H., & Tang, T. I. (2003), "Determinants of user acceptance of internet banking: An empirical study". *International Journal of Service Industry Management*, 14, 501-519.
- Luarn, P. & Lin, H. H. (2005), "Toward an understanding of the behavioural intention to use mobile banking". *Computers in Human Behaviour*, 21, 873-891.
- Ives, B. and Olson, M.H. (1984), "User involvement and MIS success: A review of research", *Management Science*, 30.5, 586-603

- Straub, D., Keil, M., & Brenner, W. (1997), "Testing the technology acceptance model across cultures: A three country study". *Information and Management*, 33, 1-11.
- McCoy, S., Galletta, F., & King, R. (2007), "Applying TAM across cultures: The need for caution". *European Journal of Information Systems*, 16, 81-90.
- Fishbein, M., & Ajzen, I. (1975), "Belief Attitude, Intention and Behavior: And Introduction to theory and Research. Reading, MA: Addison-Wesley.
- Ajzen, I. (1991), "The theory of planned behavior. *Organisational Behavior and Human Decision Processes*", 50, 179–211.
- Ajzen, I., & Fishbein, M. (1980), "Understanding attitudes and predicting social behaviour", Englewood Cliffs, NJ: Prentice Hall.
- Donahue, G. M., Weinschenk, S. & Nowicki, J. (1999), "Usability is good business", Compuware Corporation Research Report, available at: <http://www.compuware.com/intelligence/articles/usability.htm> (Accessed 17 August 2019).
- Stewart, H., and Jürjens, J. (2017), "Information security management and the human aspect in organisations", *Information & Computer Security*, vol. 25, no. 5, pp. 494–534. <https://doi.org/10.1108/ICS-07-2016-0054>
- Stewart, H., and Jürjens, J. (2018), "Data security and consumer trust in FinTech innovation in Germany", *Information & Computer Security*, vol. 26, no. 1, pp. 109–128. <https://doi.org/10.1108/ICS-06-2017-0039>.

Conclusion to STUDY 2: The hindrance of cloud computing acceptance within the financial sectors in Germany

Study 2 explored the key constructs affecting the adoption of cloud migration in enterprises. This study found that the combinations of NFC factors (data security, consumer trust and risk), technological factors (opportunity and innovation characteristics), environmental factors (government incentives) and internal-external factors (management and value creation) have a statistically significant impact on cloud adoption. These factors reinforce the positive impact of cloud migration intention.

In addition, this study has provided evidence of the role of perceived information security in adopting DT. The results show that the expectation of quality of service, security, trust and other constructs influences companies' intention to move to the cloud.

Study 2 thus reconfirms the research questions identified in Chapter 1 regarding the influence of security and trust on digital products and services.

A significant influence of promoting the cloud infrastructure does not influence its adoption, which was also explored in Study 1. Thus, the consideration of security and trust in Study 1 and Study 2 influences the intention to use digital products and services in the cloud.

However, considering the uncertainty of intangible cloud services and DT, several standards have been proposed to ensure data confidentiality, integrity and availability (CIA). Concerning the impact of DT, the question is whether industry standards can eliminate data/information security challenges, increase trust and reduce the perception of security risks. Furthermore, how does compliance with industry standards impact DT security, and to what extent does compliance with industry standards promote security? This was explored in Study 3.

Study 3 aims to explore and explicate the relationship between security and compliance with industry standards. Study 3 is presented in the next chapter.

Chapter 6. STUDY 3: Security versus compliance: an empirical study of the impact of industry standards compliance on application security

Introduction

The third study, "Security versus compliance: An empirical study of the impact of industry standards compliance on application security ", is an extension of studies 1 and 2. The aim is to explore whether industry standards can strengthen DT and IS Security. As an alternative, consider whether DT needs a different kind of security program to improve IS security despite the influence of industry standards. Alternatively, DT requires a different form of security programme to strengthen IS security even under the influence of industry standards. The aim of Study 3 is to examine the misconceptions of compliance and Security that exist in the literature.

Compliance involves meeting standards set by outside parties, such as regulatory requirements or best practices. On the other hand, Security pertains to a company's safeguards and controls for protecting its assets. It shows that a business meets the basic security standards mandated by legislative frameworks like ISO27001, TISAX, PCI, SOX, HIPAA, and GDPR.

Compliance, as opposed to Security, is motivated by business demands and is often performed to facilitate seamless business operations and to meet external regulatory obligations. On the other hand, Security is driven by technical requirements and the secure way humans interact with systems.

As discussed in Studies 1 and 2 and the literature review, compliance with an industry standard cannot guarantee data security, application security, or organisational Security. The NFC model, for example, combines numerous security operations into a unified approach to ensure adequate protection for DT and IS security. In terms of standards, ISO27001, for instance, is used to lay the groundwork for an organisation's information security, ISO27002 for implementing controls, and ISO27005, for carrying out risk assessment and risk management.

However, these standards have different characteristics: ISO27001 does not distinguish between the controls that apply to a particular organisation and those that do not, while ISO27002 requires risk assessment but does not specify the extent to which it should be conducted. Stewart (2017) concluded that the standards are different, but in combination, they lack positive features.

This study will explore the reasons behind the discrepancies between industry norms and Security. Study 3 is presented in journal article format and is currently published in the **International Journal of Software Engineering and Knowledge Engineering, published by World Scientific**. The paper's presentation adheres to the journal's guidelines, and tables and figures have been inserted strategically to make reading easier. Harrison Stewart is the sole author of the article.

<https://doi.org/10.1142/S0218194022500152>

Statement of Authorship

CO-AUTHORSHIP APPROVALS FOR HDR THESIS EXAMINATION

PUBLICATION 3

This section is to be completed by the student and co-authors. If there are more than four co-authors (student plus 3 others), only the three co-authors with the most significant contributions are required to sign below.

Please note: A copy of this page will be provided to the Examiners.

Full Publication Details	Security versus Compliance: An Empirical Study of the Impact of Industry Standards Compliance on Application Security Stewart, H. (2022), "Security versus Compliance: An Empirical Study of the Impact of Industry Standards Compliance on Application Security", International Journal of Software Engineering and Knowledge Engineering, Vol. 32. https://doi.org/10.1142/S021819402250015 .
Section of thesis where publication is referred to	All

Student's contribution to the publication	100 %	Research design
	100 %	Data collection and analysis
	100 %	Writing and editing

Outline your (the student's) contribution to the publication:

Harrison Stewart is the sole owner of this publication.

APPROVALS

By signing the section below, you confirm that the details above are an accurate record of the students contribution to the work.

Name of Co-Author 1 _____ Signed _____ Date _____

STUDY 3

Security versus compliance: an empirical study of the impact of industry standards compliance on application security

Harrison Stewart

Abstract

The integration of security aspects into software development is an open topic, especially in highly regulated industries where standards are accompanied by a high degree of complexity. Cyber attackers are constantly inventing new tools to penetrate systems and exploit even the most minor flaws, and adherence to an industry standard is not a solution. In this study, an empirical investigation is conducted over a six-month period to observe two customer relationship management (CRM) systems. To analyse

and anticipate the vulnerabilities of two CRMs, penetration testing methodologies and cross-project prediction approaches are employed. Classification using multiple machine learning approaches is utilized in the study to increase the discovery of vulnerable components in each CRM. The Student t-test is also used to assess if the mean values of the two CRM datasets are substantially different from each other in order to evaluate the efficacy of overall security and its features. The results show that security best practices during application development have a significant influence on applications created in regulated environments. The action research approach used to validate this study provided positive results and its feasibility in practice to optimise security throughout the application development. This study adds to the literature on information security management systems (ISMS) and best practices in application development in terms of creating and implementing opportunities based on broader information security management measures.

Keywords - Information security management system (ISMS); Reformed ISMS; Regulatory Standards; Technology error related information security incident; Application Security; Security sustainability

Paper type - Research paper

1.0. Introduction

Application security optimisation is constantly being researched to prevent unauthorised access to critical applications, but most of the literature in this field has not yet addressed its practical challenges (Stewart, 2020; Sahu, 2019; Calero, 2013; Sahu et al., 2014; Kumar, 2015). Even the recommendation by security experts to apply regulatory standards such as ISO27001, NIST, PCI and others has not eliminated cyber threats to applications (Stallings et al., 2012). This paper analyses the vulnerabilities of different content relationship management (CRM) systems used by two groups of organisations: One group adheres to a regulatory standard, the other does not.

Cybersecurity and regulatory standards (e.g., ISO27000 family, PCI, HIPAA, FIPPA, SOX, SOC, NIS, NIST, etc.) are two terms that are often used interchangeably (Stewart, 2017; Pavlov & Karakaneva, 2011; ISO/IEC, 2013). While cybersecurity is about detecting, preventing and preserving information assets from loss or theft, regulatory standards are concerned with risk management, often with requirements that go beyond information assets (Pavlov & Karakaneva, 2011; Safa et al., 2016; Ifinedo, 2014; Stewart, 2021; Hoffmann, 2016; Safa et al, 2016; Ifinedo, 2014; Carlson et al, 2008; Pavlov & Karakaneva, 2011; Ali et al, 2013; Stewart & Jürjens, 2017; Pavlov & Karakaneva, 2011; ISO/IEC, 2013). Furthermore, while security encompasses a set of tools and processes used to protect and defend an organisation's information and technological assets, regulatory standards focus on the storage and processing of data and the associated legal requirements or frameworks that apply to its protection (Stewart & Jürjens 2018; Luo et al., 2011; Carlson et al., 2008; Pavlov & Karakaneva, 2011; Ali et al., 2013; Stewart & Jürjens, 2017; Stewart & Jürjens 2017). Figure 1 shows the interaction between security and compliance.

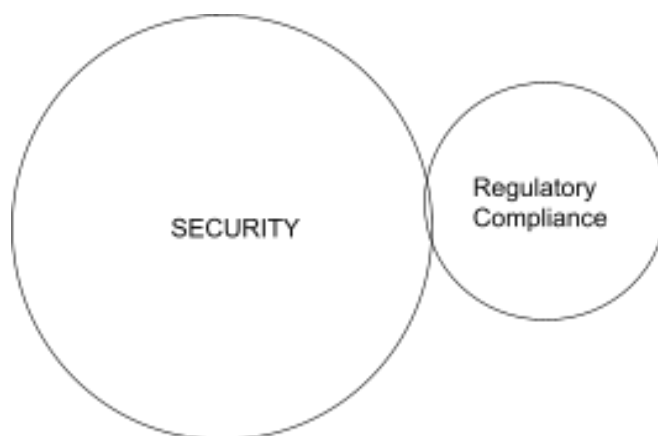


Figure 1: Interaction between security and compliance

The worldwide information security standard ISO/IEC 27001:2013 specifies the standards for an ISMS that assists organisations in managing their information security by taking humans, processes, and technology into consideration. Certification to the ISO 27001 standard is recognised globally as confirmation that an ISMS adheres to best practices in information security. ISO 27001 is a framework that assists organisations in establishing, implementing, operating, monitoring, reviewing, maintaining, and continually improving their ISMS. It is a standard in the ISO 27000 family of information security standards. Although the IS27001 is considered an industry standard for competitive advantage, it does not distinguish between the controls applicable to a particular organisation and those not applicable. (Hoffmann et al., 2016; Walid Al-Ahmad & Bassil, 2013; Ali et al., 2013; Pavlov & Karakaneva, 2011; Calero et al., 2013; Sahu et al., 2014; Kumar et al., 2015; Stallings et al., 2012; ISO, 2013). Figure 2 shows the ISMS controls according to ISO27001.

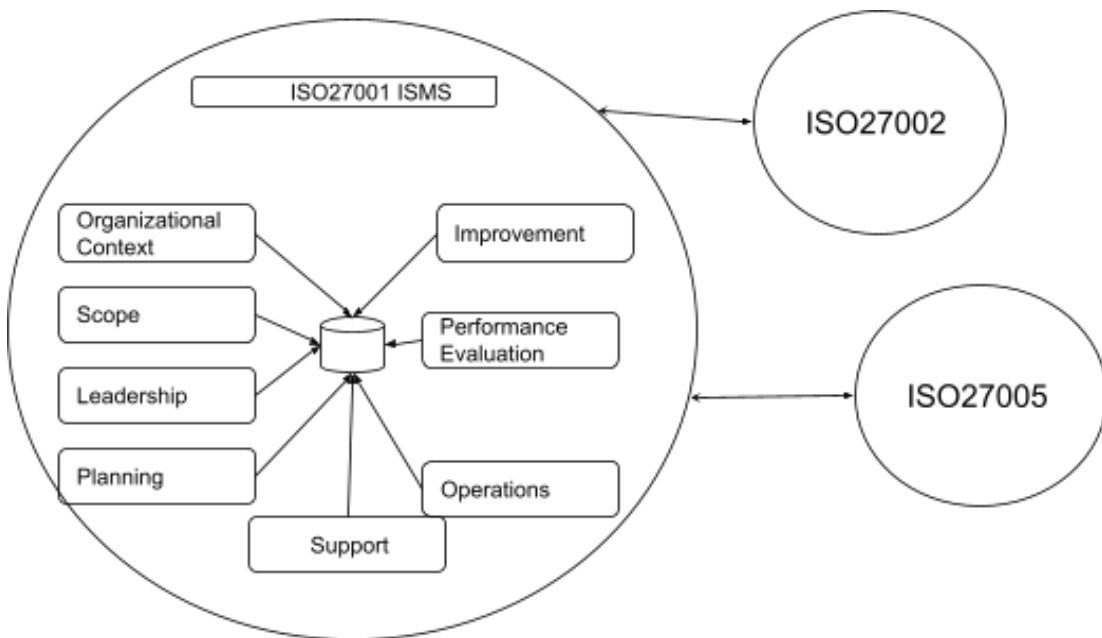


Figure 2: Information Security Management System based on the ISO27001

Unlike industry standards such as ISO27001 shown in Figure 2, application security is a combination of several factors that helps software developers develop a secure application throughout its lifecycle as shown in Figure 3 (OWASP, 2018; Kumar et al., 2015; Stallings et al., 2012; Calero et al., 2013; Sahu et al., 2014; Alenezi & Khellah, 2015). The primary approach to developing an effective and reliable

application security framework is to assess and maintain confidentiality, integrity and availability (CIA) during the application development process to prevent security breaches (Mardani et al., 2015; Luthra et al., 2015; Stewart, 2021; Calero & Piattini, 2015; Bishop, 2005; Nyanchama, 2005). A mature security framework that addresses application security must consist of (i) security by design; (ii) risk mitigation; (iii) attack and threat analysis; (iv) use and misuse cases; (v) code review; (vi) penetration testing; and (v) adherence to specific application security policies to ensure confidentiality, integrity and availability of the system and data (Calero et al., 2019; Agrawal et al., 2020). Figure 3 shows a typical application security system framework, which is completely different from the ISO27001 shown in Figure 2.

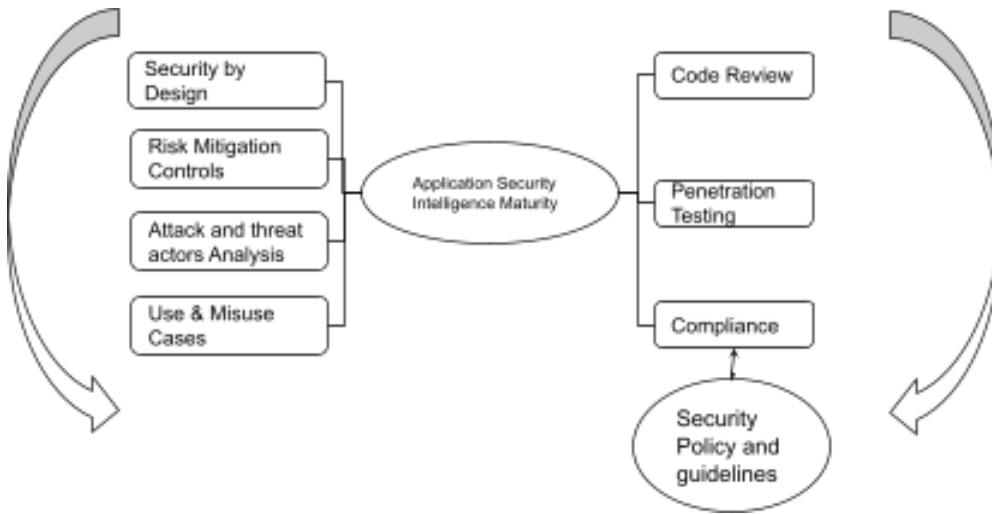


Figure 3: Application security maturity framework

As shown in Figure 4, a software application consists of several building blocks such as (i) APIs, (ii) web server, (iii) databases, (v) network configurations and (vi) application binaries. These blocks are not addressed in the ISO27001 ISMS framework shown in Figure 2.

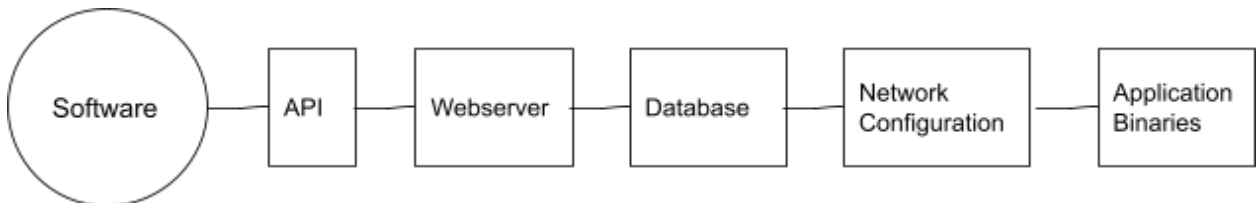


Figure 4: Software application building blocks

Hence, the link between industry standard compliance and security may be defined by identifying the capabilities that contribute to both as depicted in Figure 5.

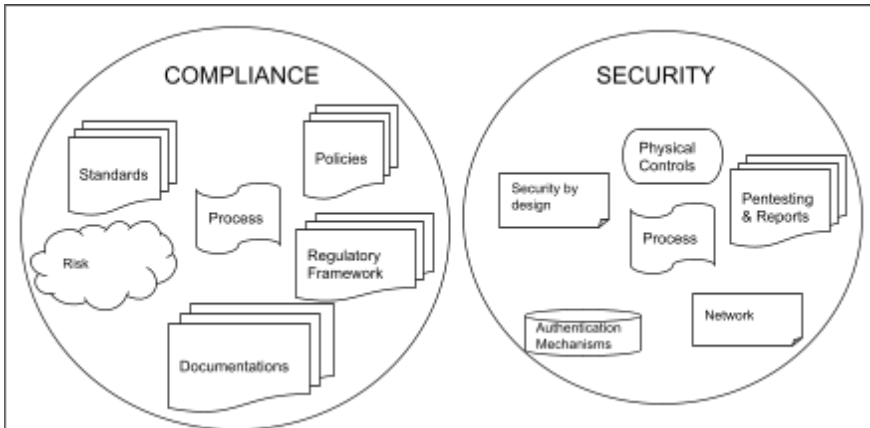


Figure 5: Components of industrial standard and application security

The study report is structured as follows: First, an overview of this study and the introduction described in part one; in section two, related work are listed. Section three examines the security of two CRM systems in two different organisations, and section four confirms the findings through data collection and penetration testing. Section five addresses the risks and limitations of validity. Section six discusses the implications of the study, followed by the conclusion in section seven. The results will help security practitioners to incorporate long-term security considerations into the application programme development process.

2.0. Related Work

The search for related work on industry standards and security was conducted in peer-reviewed security journals, conference proceedings, institutional repositories, magazines and Google Scholar. The search was conducted as in the work of Webster and Watson (2002). Table 1 provides an overview of related work.

Table 1. Related work

Study	Key Findings	Method
Moyón et al. (2018)	Suggest that regulatory requirements are utilized to generate security activities and	Literature review

	that, as a result, additional security procedures should be included while aligning them with standards.	
Fitzgerald et al. (2013)	Highlights that there is a lack of agile methods in regulated environments, which leads to security shortcomings.	Continuous Software Engineering (CSE)
Bartsch (2011); Baca (2012); Beznosov & Kruchten (2004); Siponen et al. (2005); Felderer & Pekaric (2017)	The authors concentrate on solving security issues without focusing on regulations.	Literature review
Felderer & Pekaric (2017); Bell et al. (2017); Ahola et al. (2014); Baca & Carlsson (2011); Ch'oliz et al. (2015); Baca et al. (2015); Stephanow & Khajehmoogahi (2017)	Propose the integration of security into the application development process and neglect standards compliance activities.	
ISO/IEC (2017)	Propose a holistic approach to combine safety and industry regulations for an in-depth analysis of a safety standard.	S ² C-SAFe Scaled Agile Framework (SAFe).
Bartsch (2011)	Suggest practical concerns of continuous -security procedure	S ² C-SAFe

	during development process to security.	
Tøndel et al. (2017)	Propose an approach to bridge the gap between application development, practical security and compliance.	S ² C-SAFE
Beck et al. (2011)	Highlights that application development requires individual assessment and collaboration, while standards focus on documentation, agreements and a defined process	Survey
Calero & Piattini (2015)	Suggest avoiding laxity in security and sustainability when developing a web application for an institution where data, time, and big assets are at stake.	Sustainability on design features.
Schieferdecker (2020)	Suggests that developers need to pay attention to sustainability and security simultaneously to ensure that the software is both sustainable and secure.	Ethical principles for software development.
Stewart (2020)	Address security and protection issues in organisations and suggest that work should focus on malware code development and improving the framework for accessing applications.	
Stewart (2021) Stewart (2020)	Recommend that sensitive data stored on cloud servers be	

	encrypted before being stored in the cloud.	
Agarwal et al. (2019)	The study uses fuzzy based MCDM approach and multi criteria decision making approaches to identify four parameters that are very important to ensure application security, namely: confidentiality, integrity, availability, and durability.	Fuzzy based MCDM approach.
Calero & Piattini (2019)	The results of the study show that durability as a sustainability characteristic and binding, cohesion of design attributes as essential characteristics that have a significant impact on the security of the web application.	Human, Environmental and Economic sustainability.
Oyedeji et al. (2018)	Suggest that developers need to look at sustainability and security simultaneously to ensure that the software is both sustainable and secure.	Catalog of web application sustainability designs
Venters et al. (2018).	Suggest research methods to show how to deal with sustainable security in software architectures.	Software security and sustainability Architectures
Li et al. (2017)	Developed a new strategy for mobile edge computing based on a security framework using fuzzy theory	Fuzzy theory
Babak et al. (2015)	The results of the study show the most important risks of web	Mapping severity of Confidentiality, Integrity and Availability (CIA).

	applications that must already be considered in the planning phase.	
--	---	--

3.0. Background

Two CRM software vulnerabilities were investigated at two companies, involving remote code execution, denial-of-service (DoS) attacks, cross-site scripting (XSS), SQL injection and cross-site request forgery (CSRF). Company A and Company B are two distinct companies operating in the three main service and utility sectors traditionally managed by the public sector: Water Management, Waste Management and Energy Services. Company A has more than 419,922 employees in 72 countries of different nationalities and company B has more than 19,748 employees in 30 countries. Company B's software development department does not comply with ISO27001 or any other relevant industry regulation, while Company A complies with ISO27001 certification and other standards. The two firms are among the fastest growing innovative companies over the last decade: Current production is 2.1 million and 1.7 million sales per day, respectively; net profit was over 6.8 billion euros and 4.8 billion euros in 2020.

All their areas are very complex and require a variety of activities and professional enterprise applications for processing sensitive data. They bring together experts from different disciplines and with mutual knowledge on an exceptionally global scale. Compliance with the General Data Protection Regulation (GDPR) is also critical to all the two companies, not to mention the legal and policy regimes that have given the sectors confidence in their data. The challenge, then, is to integrate the various information security disciplines within the software development department and ensure a balance between the efficiency required for routine activities and the innovation required for new projects.

The companies develop their own application programmes, all based on modern technology, to satisfy their customers and gain their trust (Stewart 2021; Stewart & Jürjens, 2018). Large amounts of sensitive data are processed here. Company A's public image seems to be good as it can convince customers and partners with its ISO27001 certification and other standards. In contrast, Company B is still in the process of preparing for ISO27001 certification. However, company B has created an application security framework that governs how developers should develop its enterprise application.

This sparked interest in studying the two CRMs to predict which of them are vulnerable to cyber-attacks and whether or not the applications, developed in an industry-standard environment, convey security.

After meeting with the CIOs of each company, it became apparent that the software developers of company A were not trained in application security development compared to company B. The average score for application security awareness among the developers of each company is shown in Table 2.

Table 2. Application security awareness among developers

	Overall awareness (%)	
	2019	2020
company A	0.1%	0.2%
company B	99.9%	99.8%

4.0. Methodology

This work makes a two-fold contribution: it evaluates two firms through surveys and penetration testing. Here, a survey was conducted initially, followed by a pilot test, interviews, data analysis, penetration testing (Kali, 2014; Owasp, 2019; Duan et al., 2019; Zhou 2020; Kumar et al., 2019; Walsham 2006), cross-project vulnerability prediction (Kawata et al., 2015; Hosseini et al., 2016; Bin et al., 2017; He et al., 2018; Herbold et al., 2018), hypothesis testing (O'Mahony, 1986) and observations perspective (Baskerville's, 1999). The research method is shown in Figure 6.

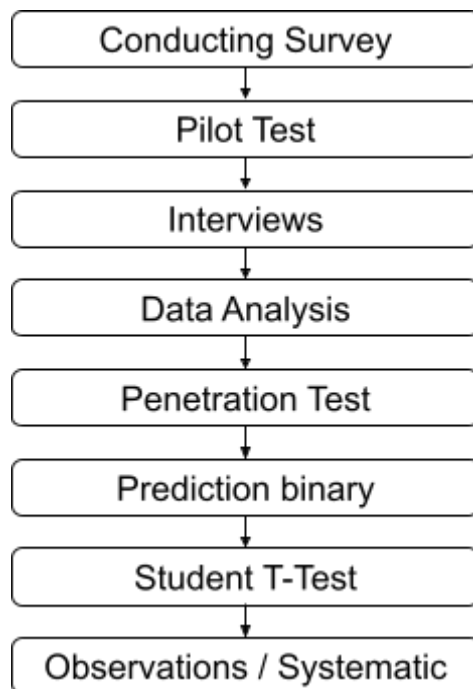


Figure 6: Research methodology

In this study, vulnerability prediction is framed as a classification issue by predicting if Company A CRM system is vulnerable. This study presents a cross-project vulnerability prediction framework to automatically predict vulnerabilities in the two CRMs. The proposed approach is shown in Figure 7. Based on the source code metrics of both CRM files and their class labels (vulnerable or not vulnerable), the predictive model is trained on the two data. After running the model on this training dataset, it is tested on a third project to evaluate the effectiveness of this model in predicting the vulnerabilities of another project (cross-project prediction). Cross-project vulnerability prediction models are trained on data from one or more projects for which predictors (e.g. product metrics) and actual vulnerabilities are available. Predictive models are then built using machine learning techniques (classifiers) to predict vulnerabilities in the application program files of a new project. To further test the hypotheses of whether compliance conveys security or not, student t-tests (O'Mahony, 1986) are used as the approach for this study.

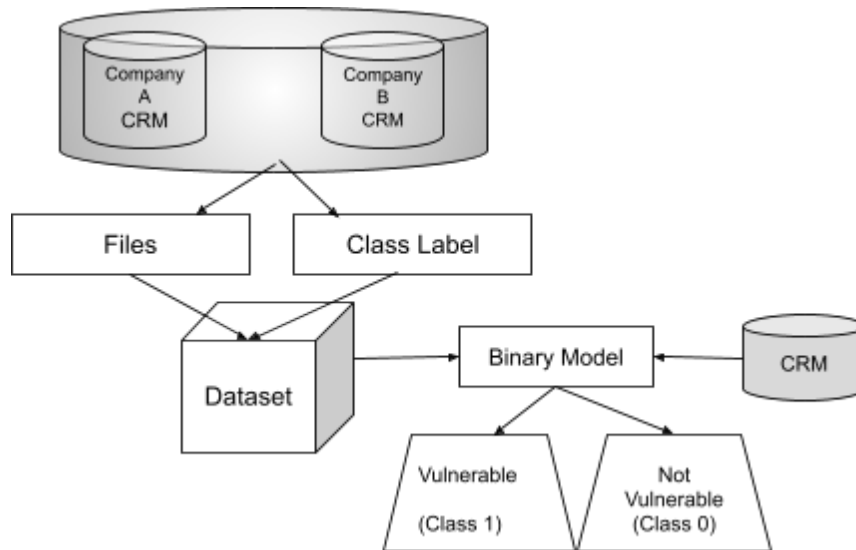


Figure 7: The conceptual prediction binary classification approach.

Following Baskerville's (1999) approach to testing and refining this case study, the five-month action research consisted of two research cycles. The first phase of research in both sectors started from March 2020 to May 2020 and consisted of interviews and application testing. The second phase, also referred to as the observation phase, began in May 2020 and was completed in September 2020. This second phase focused on improving security through development and communication.

4.1. Survey Data Collection

The representative sample technique was used for the survey so that the study's findings could be confidently extrapolated. A data policy agreement was signed; which stated that the data collected would be utilized only for this study and would not be imparted to any third party.

The data collection phase was conducted in three steps, as in the work of Walsham (2006), namely: (1) a survey, (2) interviews and (3) participant observation. An anonymous and open-ended survey was used to collect information about software developers' knowledge of information security in relation to security in development with established policies, their behaviours, opinions and their application development process to maintain application security. The survey was conducted anonymously by telephone, by mail, via the Internet and in person to obtain more honest feedback (Myers and Newman 2007; Walsham 2006). Data analysis was conducted using the SPSS programme. Questionnaires were completed using the Cetbix situational awareness platform.

The pilot test in the initial phase consisted of 37 questions. In the final version, 26 questions were asked based on the feedback from the pilot test. During the pilot test, a selected group of staff tried out the 40 tested questions and gave their feedback before the final questions were fully deployed. The interviews lasted 45 minutes.

Semi-structured interviews were then conducted to gain a deeper understanding of developers' perceptions and opinions of application security compliance versus regulatory standards during development, particularly with regard to their current practices and their ability to use their current information security policy (ISP) or other application security policies directives. Open-ended questionnaires were used during the interview (Britten, 1995). The interview started with questions that the participants could easily answer and then moved on to more difficult and sensitive topics. This helps to make respondents feel comfortable, build trust and rapport (Stewart & Jürjens 2018), and generate rich data with which to subsequently develop the interview (Britten, 1999).

The data collecting phase was conducted with the direct involvement of personnel and the ISP programme manager. All of the questions were related to one of the items in Table 3. These related items are standard items from the Cetbix Risk Assessment Tool used to conduct the survey. The abbreviation "Q" in Table 3 represents the number of questions in each of the related items selected for this work.

Table 3. Questionnaire and related questions

Related Items	Questions
General questions	Q1- Q11
Mitigation Strategies to Prevent Malware Delivery and Execution	Q12- Q18
Mitigation Strategies to Limit the Extent of Cyber Security Incidents	Q19 - Q21
Mitigation Strategies to Detect Cyber Security Incidents and Respond	Q22- Q23
Mitigation Strategies to Recover Data and System Availability	Q24 - Q25
Mitigation Strategy Specific to Preventing Malicious Insiders	Q26

The survey, interviews, and observation provided insights into the information security strategies of all the three companies. Also examined were (i) the extent to which development teams are aware of risks associated with deprecated protocols and cryptography, (ii) security information based on detailed knowledge of the current security posture of their CRM applications, (3) cyber threat information shared among colleagues and partners, (4) organisational commitment to application security development projects, and (5) misconceptions about application security based on security expertise and knowledge. Systematic sampling was used to select respondents (see Table 4).

Systematic sampling based on picking every n th person where $n = \frac{\text{population size}}{\text{sample size}}$ (1)

In both firms, there were 30 IT employees. Each number was divided by ten, yielding a total of three. Every third individual was chosen here. As a result, the sample size was reduced to ten persons. Each interviewee was issued an anonymous ID identification to maintain anonymity (Walsham 2006), as indicated in Table 4.

Table 4. Employee Tags Used for Anonymity

Group of users	Number of users company A	Number of users company B	Anonymous ID
CTO	1	1	IDR_SE1
Senior Developer	3	3	IDR_SD
Junior Developer	6	3	IDR_JD
Security Teams	0	3	IDR_ST
$n =$	10	10	

As mentioned earlier, the data collection in this study consists of a survey and a penetration test. After surveying the two companies, the next step was to subject all the CRM systems to a penetration test to identify exploitable vulnerabilities and to verify if company A CRM system is vulnerable. The dataset collected during penetration testing is described in Section 4.2.

4.2. Penetration Testing (Dataset)

In this study, data is collected from all the CRMs, as in the work of Walden et al. (2014). The data contains various software metrics and vulnerability information about their CRM files. This dataset was collected through penetration testing performed by 6 ethical hackers (Tounsi & Rais, 2018). A penetration test is a simulated cyber attack on a computer system, network, website and application program to discover exploitable vulnerabilities (Tufan et al., 2021; Al-Matari et al., 2020). It is considered a legal and authorized measure to assess and secure computer networks. (Kali, 2014; Owasp, 2018; Owasp, 2019; Khater et al, 2020; Tounsi & Rais 2018). For this purpose, a vulnerability scanner is used to verify the security of the CRM systems to detect vulnerabilities and security holes (Kali, 2014; Duan et al., 2019; Zhou 2020). Most advanced vulnerability scanners rely on a vulnerability database that includes information related to services, packet types, ports and other known vulnerabilities that pose a threat as well as recommendations for addressing those vulnerabilities (Agrawal et al., 2019; Calero & Piattini, 2019).

In addition, the researcher and the ethical hackers used attack simulations, malicious attack techniques, and a system security status assessment for penetration testing of the network servers running the CRM system. The steps to develop the pentest are based on the approach of Vaca et al. (2020). Their work sheds more light on the phases of penetration testing in the pre-attack phase with passive exploration and active exploration. Throughout the assessment process, the researcher and the six pentesters followed the proactive approach to exploiting the vulnerability from an attacker's perspective, which relies on active analysis of different vulnerabilities, technical flaws and system weaknesses.

All these tests were conducted by six different professional ethical hackers to minimise the amount of subjective opinion in each measurement. To avoid any bias in the validation, the size of each organisation's attack surface, such as the network attack surface, the application program (CRM) attack surface, the physical attack surface and the security awareness of the CRM users were taken into account (Tufan et al., 2021).

For the attack surface of their network, the overall design/topology of the network, open ports, insecure protocols, multiple users with management account, low bandwidth, placement of critical systems, firewall rules and other security mechanisms such as Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) and Virtual Private Network (VPN) were considered (Tufan et al., 2021). The researcher and pentesters observed the size of the organisations' internal networks and multiplied it by the size of their internet presence. For the attack surface of the applications, the number of running services, the number and type of ports the applications listen to, privacy settings, open-source application programs, application programs without security updates and their patch management were taken into account (Owasp, 2018; Owasp, 2019; Al-Khater et al., 2020).

Furthermore, since employees play a major factor in application security, employee's attack surface, such as the risk from social engineering, potential for human error, rogue devices, passwords on sticky notes, phishing emails, and the risk of malicious conduct were addressed (Stewart, 2020; Al-Khater et al., 2020).

After assessing all these areas, the extent of each organisation's attack surfaces, their level of exposure, their vulnerabilities and how an attacker could exploit them was known (Al-Matari et al., 2020). All of these assessments enabled the mapping of all touch-points between any host on the Internet and any host on each respective organisation's internal network. These touch-points included user interface forms, HTTP headers and cookies, APIs, files, databases and other local storage, emails and other messages, and run-time arguments. These touch-points are considered vulnerable paths for attackers to penetrate an organisation's network or attempt to exfiltrate data (Tufan et al., 2021; Al-Matari et al., 2020).

The six ethical hackers and the researcher also identified the CRM processes, transaction interfaces/APIs, operational commands, monitoring interfaces/APIs, and interfaces to other applications/systems. They also examined attack vectors such as SQL injection, DDoS attacks, phishing attacks, and eavesdropping attacks. Each CRM system risk was classified as low risk, medium risk, or high risk (Vaca et al., 2020; Jouini et al., 2014). This work took into account the attack surfaces of each organization to ensure transparent validation. Applications that do not belong to the two organizations were separated from the target application. Unassigned and non-registered IP addresses were blocked from accessing the application's networks. Other regions and countries not associated with these organizations were also blocked from accessing the application. Those irrelevant regions, IPSs, and malicious websites were not worth the required firewall and IPS resources, nor a flood of security

incident and event management (SIEM) alerts (Vaca et al., 2020). In other words, the researcher and the hackers filtered out these issues to save security resources by examining only the truly unknown traffic and focusing on what was important, not what was already known.

While this pentesting was intended to allow researchers to evaluate the CRM, it was also necessary to ensure that the test did not disrupt the normal operation of the business system. Tools used in the penetration testing include but are not limited to nmap, burp-suite and metasploit (Walden et al., 2014). The in-depth study of both systems provides a comprehensive understanding of the nature of cyber attackers and their threats (Al-Khater et al., 2020). The attack phase included various methods. All tests were conducted in a phased manner according to the National Institute of Standards and Technology (NIST SP 800-115) (Scarfone et al., 2008).

Tables 5 and 6 reflect the severity rating in the test report for Company A and Company B, respectively. To statistically measure the severity of a vulnerability, the Common Vulnerability Scoring System (CVSS) is used to provide a numerical score of measurement. To simplify this measurement, the risk level is stated in descending order of criticality as high, medium, and low. Any deviation from associating a vulnerability with the standard rating is documented and justified by the penetration testing team. The penetration testing team documents and justifies any divergence from the conventional attribution of a vulnerability to a rating. These results will be used in the next sections to further evaluate this paper.

Table 5: CVSS results of the penetration test for company A

	High	Medium	Low	Total
Hacker 1	10	2	2	14
Hacker 2	17	1	1	19
Hacker 3	11	2	4	17
Hacker 4	12	3	1	16
Hacker 5	13	4	1	18
Hacker 6	11	1	2	14
Total Vulnerabilities				98

Table 6: CVSS results of the penetration test for company B

	High	Medium	Low	Total
Hacker 1	0	0	1	1
Hacker 2	0	0	1	1

Hacker 3	0	0	1	1
Hacker 4	0	0	1	1
Hacker 5	0	0	1	1
Hacker 6	0	0	1	1
Total Vulnerabilities				6

The dataset, which contained various software metrics and information about vulnerabilities in the files, was collected from both CRMs and examined by the researcher and ethical hackers. Table 5 provides descriptive statistics on the dataset.

Table 7: Descriptive statistics on the dataset of the two CRMs

System	Vulnerable Files	Total files	Standard Compliant
company A - CRM	98	1631	Yes
company B - CRM	6	3731	No

Table 8 and 9 show the number of connections made by each ethical hacker. For consistency, the intervals were set to the default of 10 seconds with a test connection timeout of 5 and a test duration of 240 seconds. Each ethical hacker was asked to perform a DoS attack based on the default settings to determine how many connections would succeed and at what number of connections the server would become unreachable. As shown in Table 8, 99% of the DDoS attacks at Company A resulted in a noticeable disruption to the CRM system, which was not the case at Company B, as shown in Table 9. These results will be used in the next sections to further evaluate this paper.

Table 8: Results of the DoS attack for company A

Number of connections	Intervals/sec	Probe connection Time Out	Test duration/seconds	Connected	Pending	Server Down
2000	10	5	240	1900	2100	Yes
2000	10	5	240	1901	2200	Yes
2000	10	5	240	1911	1905	Yes
2000	10	5	240	1161	100	Yes
2000	10	5	240	1000	1011	Yes

2000	10	5	240	1800	1702	Yes
------	----	---	-----	------	------	-----

Table 9: Results of the DoS attack for company B

Number of connections	Intervals/sec	Probe connection Time Out	Test duration/sec	Connected	Pending	Server Down
2000	10	5	240	10	0	No
2000	10	5	240	10	0	No
2000	10	5	240	10	0	No
2000	10	5	240	10	0	No
2000	10	5	240	11	0	No
2000	10	5	240	10	0	No

4.3. Experimental Design

The researcher further explored which of the two systems would be a suitable fit for the training dataset. In this study, the predictive model in Figure 6 relies on existing classifiers to investigate which of these CRM systems are appropriate for the training dataset. Using data mining techniques on software metrics is one approach for automatically predicting vulnerabilities. The model learns from training data and predicts class labels for any given data (Kawata et al., 2015; Hosseini et al., 2016; Bin et al., 2017; He et al., 2018; Herbold et al., 2018).

There are several classification algorithms, and it is difficult to predict which method is superior to another. The selection of one of these methods depends on the application and the nature of the data set at hand. In this study, five algorithms' methods, namely logistic regression (Hilbe, 2009), Naive Bayes (Lewis, 1998), J48 decision tree algorithm (Quinlan, 2014), Random Forest (Chan and Paelinckx, 2008), and Support Vector Machines (Hearst et al., 1998), are used to build a vulnerability prediction model in Weka (Hall et al., 2009). In machine learning, the process of predicting the class of data points provided is called classification. These classes are also referred to as targets, labels, or categories. This classification aims to estimate the accuracy of each target class for each data sample (Kawata et al., 2015; Hosseini et al., 2016; Bin et al., 2017; He et al., 2018; Herbold et al., 2018). A classification task starts with a collection of training datasets and requires the use of machine learning algorithms to

figure out how to assign class labels to instances, e.g., "vulnerable" or "not vulnerable." There are a variety of

classification tasks, namely: predictive modeling, binary classification, multi-class classification, multi-label classification, and unbalanced classification.

Since the model is based on two instances: "vulnerable" or "not-vulnerable", binary classification is chosen in this work. Moreover, the five algorithms selected for this work match the binary classification. Here, "not vulnerable" is the normal state with class label 0, while "vulnerable" is the abnormal state with class label 1 as shown in Figure 6.

4.4. Evaluating The Predict Measures

The classification algorithm is evaluated based on F-measure, recall and precision. F-measure provides a precise description of the classifier, Recall evaluates the extent to which vulnerable classes (instances) are covered by a model and Precision measures the actual number of vulnerable instances returned by the model. A high recall value means less false-negative results (Neuhaus et al., 2007) while a high precision value means less false positives. Since neither precision nor recall provide reliable results when used alone, the F-measure in this study was intended to provide a way to represent both aspects with a single result. F-Measure combines precision and recall into a single metric that accounts for both characteristics (Powers, 2011). Based on the binary classifier, two errors were expected, i.e., false positive (FP) or false negative (FN). For the two classes - vulnerable or not-vulnerable - the vulnerable classes are classified as true positive (TP) and the non-vulnerable classes as true negative (TN). The confusion matrix in Table 10 provides information about the individual - vulnerable or not-vulnerable - performance measures.

Table 10: Confusion Matrix

	Positive Prediction	Negative Prediction
Positive Class (not-vulnerable)	True Positive (TP)	False Negative (FN)
Negative Class (vulnerable)	False Positive (FP)	True Negative (TN)
	Vulnerable CMR (company A)	Not Vulnerable CRM (company B)

The confusion matrix highlights the performance of the prediction model and the accuracy of the class predictions (vulnerable and not vulnerable), as well as the associated errors.

$$\text{Recall} = \frac{\text{True Positive (TP)}}{\text{True Positive (TP)} + \text{False Negative (FN)}} \quad (2)$$

$$\text{Precision} = \frac{\text{True Positive (TP)}}{\text{True Positive (TP)} + \text{False Positive (FP)}} \quad (3)$$

$$\text{F-measure} = 2x \frac{\text{True Positive (TP)}}{\text{True Positive (TP)} + \text{False Positive (FP)}} \quad (4)$$

4.5. Precision Results

Based on the results for precision, recall, and F-measure, the Random Forest and J48 classifiers outperform logistic regression, Naive Bayes, and Support Vector Machines, as shown in Table 11. Table 11 displays the performance of the classifiers as well as the relevant assessment measures. Random Forest and J48 fared similarly with some fluctuation, but Random Forest outperformed J48. That is, in the case of company A's dataset, F-measure values for NB, LR, J48 and RF, are 0.736; 0.739; 0.787 and 0.755 respectively while company B's F-measure values are 0.948; 0.989; 0.981 and 0.995 respectively. The results indicate that J48 and RF classifier techniques outperformed NB and LR based on Precision, Recall, and F-measure. The proportional odds assumption (ordinal logistic) is then used to test whether the difference between J48 and RF is significant in building predictive models. The proportional odds assumption (ordinal logistic) was preferred to the Kruskal-Wallis test [Sprenst and Smeeton, 2007] because Kruskal-Wallis does not indicate the groups that differ, only whether a significant difference exists between them. These results are shown in Table 11.

Table 11: Classification outcomes

	Naive Bayes (NB)	Logistic Regression (LR)	Support Vector Machines (SVM)	J48	Random Forest (RF)
company A					
Recall	0.739	0.721	0.746	0.775	0.747

Precision	0.734	0.729	0.717	0.739	0.739
F-Measure	0.736	0.739	0.759	0.787	0.755
company B					
Recall	0.971	0.991	0.991	0.993	0.994
Precision	0.985	0.985	0.984	0.986	0.986
F-Measure	0.948	0.989	0.989	0.981	0.995

The ordinal logistic test was conducted separately for the F-measures, as shown in Table 12. The p-value exceeds 0.05, indicating that the difference in F-measure values is not clinically meaningful.

Table 12: Proportional odds assumption (ordinal logistic) of J48 and RF outcome

	F-measure
<i>chi-squared (χ^2 test)</i>	2.0
<i>Degrees of freedom</i>	2.1
<i>p-value</i>	0.3796

The model was trained on the CRM dataset of company A, as its vulnerability distribution was greater than that of company B's CRM dataset. The results of the cross-project prediction are presented in Table 13. The outcomes proved reliable. Small discrepancies in performance between the cross-project prediction and the within-project prediction were also observed.

Table 13: Cross Project Prediction Results

	J48	RF
Precision	0.986	0.985
Recall	0.957	0.949
F-Measure	0.969	0.952

The F-measure in company A's CRM dataset for within-project and cross-project prediction is 0.011, as seen in Figures 8 and 9 based on J48 and RF.

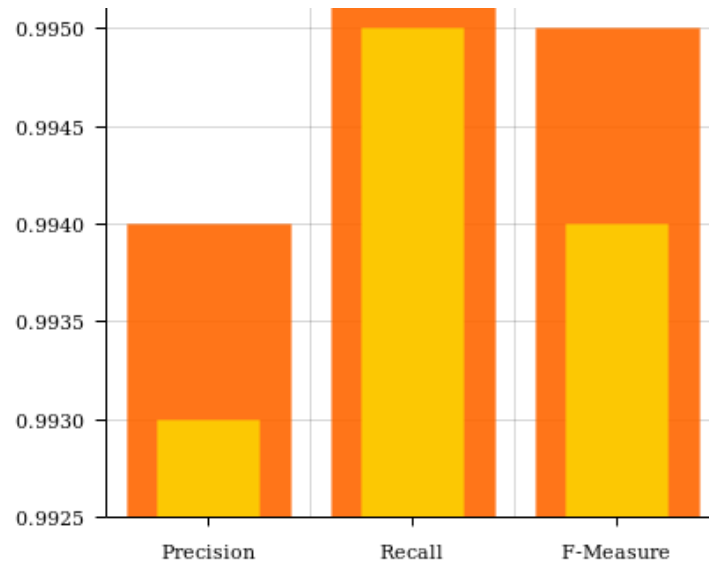


Figure 8: Within-project vs. Cross-project model performance (J48)

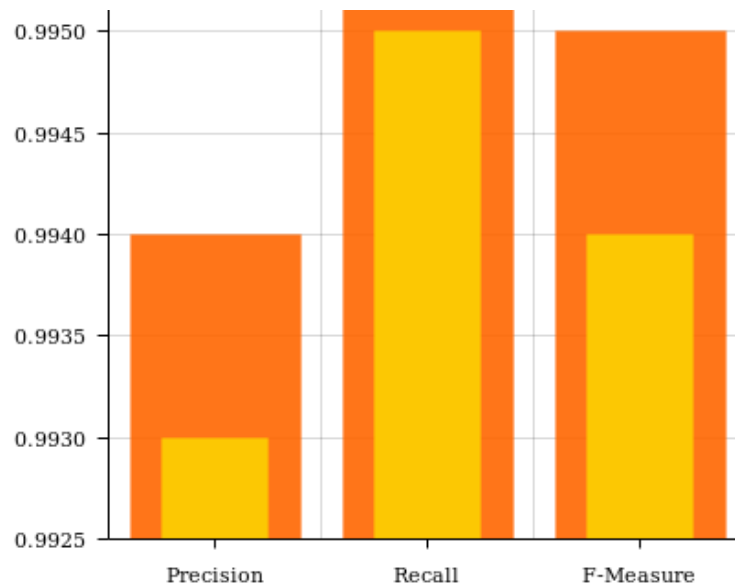


Figure 9: Within-project vs. Cross-project model performance (RF)

At this point, it is clear that company A's industrial compliance framework has no impact on the development and security outcomes of its CRM system. The next step was to analyse whether compliance with the standards has an impact on the network and systems running the CRM. For this, the student t-test is used to answer hypotheses.

4.6. Validation of Penetrations & DOS Attack

Based on the results in Table 5, 6, 7 and 8 the discrepancies in the vulnerability of the two CRM systems were normalised by the number of internal systems in the network of both organisations. To eliminate any variations between systems, the number of systems in each organisation was divided by the number of intrusion attempts and DoS/DDoS connections. The two sets of data from the two companies are evaluated by formulating the following hypotheses:

- **H0:** There is no difference between company A's and company B's datasets and applying additional application security policies rather than compliance with a regulated standard has no application security implications.
- **H1:** There is a significant difference between company A's and company B's datasets and applying additional application security policies rather than compliance with a regulated standard has application security implications.

The hypotheses are tested using the student t-test (O'Mahony, 1986). The two main output parameters of this student t-test are the t-statistic and the p-value. Similar to the normality test of D'Agostino and Pearson (1973), the conclusions to accept or reject the null hypothesis are based on the magnitude of the p-value. To minimise the possibility of error, the p-value was set at 0.01 (i.e., a 99% confidence level) rather than the recommended level of 0.05 (i.e., a 95% confidence level). The probability of error in rejecting H0 was assumed to be 1 %.

The t-statistic is calculated as follows:
$$\frac{\bar{X}_1 - \bar{X}_2}{s_p \sqrt{\frac{2}{n}}} n \tag{5}$$

where n = number of observations, \bar{X}_k = the mean value of dataset k , $s_p = \sqrt{\frac{S_{X_1}^2 + S_{X_2}^2}{2}}$ - unbiased estimator of variance of the k -th dataset.

The central limit theorem is used to normalise the distributions (Bárány and Vu, 2007) by iteratively sampling each data set and calculating the means at each iteration of 100 iterations with 30 values in each sample. The distributions appear as indicated in Figure 10 a, b, c and d respectively:

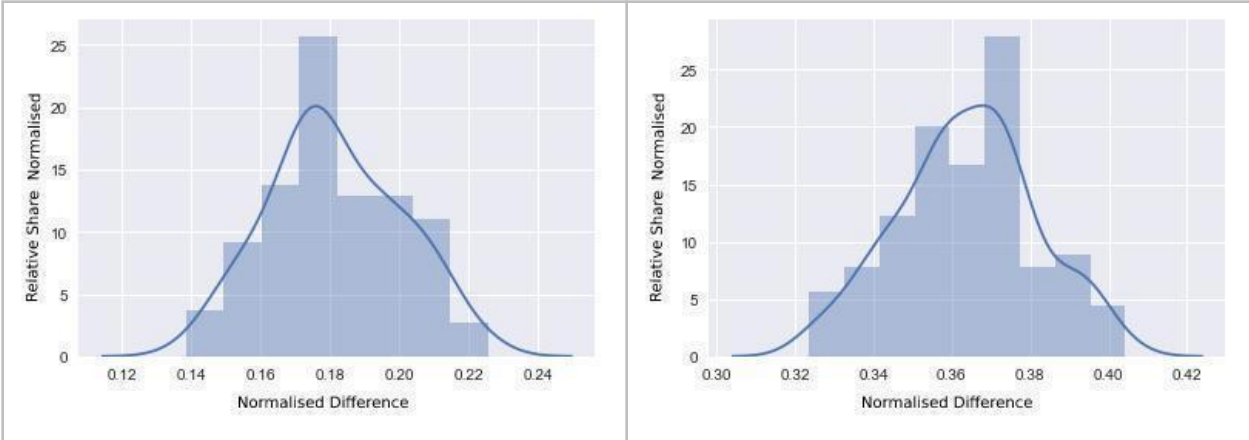


Fig 10: a. Mean distributions of penetrations for Company A

Fig 10: b. Mean distributions of penetrations for Company B

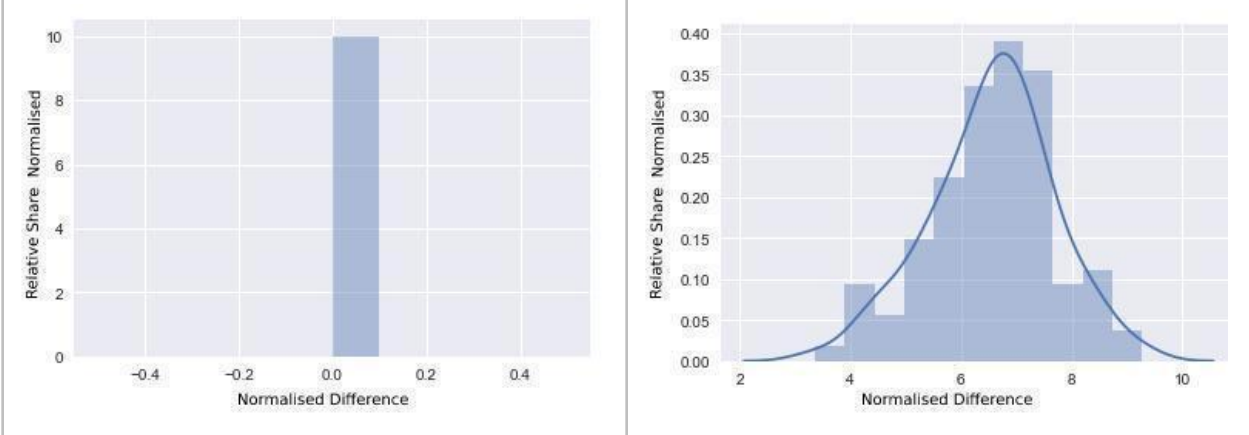


Fig 10: c. Mean distributions of DoS for company A

Fig 10: d. Mean distributions of DoS for company B

Fig.10. a shows the normalised distribution of average differences per system for penetrations for Company A, while Fig.10. b shows the normalised distribution of average differences per system for penetrations for Company B. Fig.10 c shows the number of allowed connections during DoS/DDoS attacks for company A, while Fig.10.d shows the number of allowed connections during DoS/DDoS attacks for company B. After testing the normality hypothesis, the following results were obtained (see Table 14).

Table 14: Normality tests after CLT is applied

	K-statistic	p-value
--	-------------	---------

Mean distribution of penetrations difference company A	2.44	0.29
Mean distribution of DoS attacks connected differences company A	Null	1.0
Mean distribution of penetrations difference company B	0.41	0.81
Mean distribution of DoS attacks connected differences company B	1.6	0.45

As shown in Table 14, the p-values are high (above the value of 0.1) in all four cases. This indicates that the distributions are normal and student's t-test can be used to compare the measurements.

Furthermore, it was possible to calculate the p-value with a significance level of 99 % based on the number of degrees of freedom. The t-statistic for penetration testing is -68.8, with a corresponding p-value of approximately 3.4068e-140, which is extraordinarily low. This number is significantly lower than the previously stated threshold, implying that the H0 hypothesis can be rejected. In this case, company A's negative t-statistic value is larger than that of company B. This implies that conformity does not convey security, allowing the H1 hypothesis to be accepted.

The uninterrupted capabilities of both CRMs are then examined by evaluating the amount of DoS attacks using the following hypothesis to see if conformance has an influence on security.

- **H0:** There is no difference between company A's and company B's number of external connections allowed and applying additional application security policies rather than compliance with a regulated standard has no security implications.
- **H1:** There is a significant difference between company A's and company B's number of external connections allowed and applying additional application security policies rather than compliance with a regulated standard has security implications.

The operations lead to the following results:

$$T\text{-statistic} = -71.88, p\text{-value} = 3.018e-87 \tag{6}$$

Since p-value is significantly smaller than the specified threshold of 0.01, the H0 hypothesis can be rejected once more. This implies that compliance does not imply security, allowing the H1 hypothesis to be accepted.

4.7. Combined Validation

A further hypothesis test is conducted for the number of penetrations and the number of connections permitted, and the H0 hypothesis is rejected again owing to its low p-value in both situations. A final

hypothesis test was performed for the combined distributions of penetrations and DoS attempts to achieve more certainty in answering the research question.

- **H0:** The combined distributions do not differ and applying additional application security policies rather than compliance with a regulated standard has no security implications.
- **H1:** The combined distributions differ and applying additional application security policies rather than compliance with a regulated standard has security implications.

The first stage was to determine the degree to which the two factors were dependent on each other for both firms. The covariance is determined for this purpose as follows:

$$Cov_{XY_{before}} = 3.22e - 04, Cov_{XY_{after}} = 3.16e - 08 \quad (7)$$

Both covariances are low, indicating that the variables are independent. The following basic parameters can be calculated:

$$\frac{X -}{comb} = \frac{X -}{1} + \frac{X -}{2} s_{comb} = \sqrt{s_1^2 + s_2^2 + 2Cov_{12}} \quad (8)$$

where X_i is the sample mean and s_i is the sample standard deviation.

After determining the parameters of the combined distributions for the differences between companies A and B, the values are simulated using the Monte Carlo method before further hypothesis testing (Anderson, 1986). In accordance with the parameters of the normal distribution for each combined variable, 100 independent random values are generated. These 100 independent values represent the state of security for company A and company B separately. The hypothesis test is performed on the generated states of security and the process was iterated 10,000 times. The distribution of the t-statistics is shown in Figure 11.

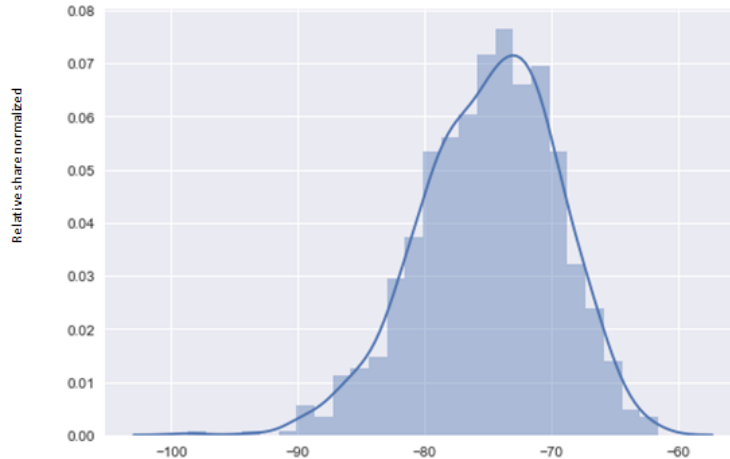


Figure 11. T-statistics distribution of 10,000 generations

As shown in Figure 11, the t-statistic for the average of the combined cases is -72.4, and the corresponding p-value is $1.06e-142$ on average. Since there is no significant difference in the t-statistic and p-value, H_0 is rejected without any doubt due to the extremely low p-value, which ultimately answers the research question that industry compliance frameworks (e.g. ISO27001, NIST, PCI) have no impact on application security development and outcomes.

The results of the study were preliminarily confirmed using different approaches and showed a solid consistency between the hypothesised properties and the associated information. To be sure that there is a significant influence of the application security strategy on the application results, three different hypotheses were tested using t-test as follows:

1. Hypothesis tests for the mean number of penetration differences.
2. Hypothesis test for the mean number of permissible connection differences during the DoS attack.
3. Combined hypothesis tests for the mean number of penetration differences and the mean number of permissible connection differences.

In all three cases, the hypotheses have been formulated as follows:

- H_0 : The application of application security measures has no impact on application security in comparison to regulatory standards (ISO27000 Family, PCI, HIPAA, FIPPA, SOX, SOC, NIS, NIST, etc.).

- H1: The application of application security measures has a significant impact in comparison to regulatory standards (ISO27000 Family, PCI, HIPAA, FIPPA, SOX, SOC, NIS, NIST, etc.).

4.8. Observation

The method of this observation is based on a systematic approach. In doing so, the researcher focused on different types of activities to highlight the distinctions in this study (Angrosino & dePerez, 2000). Due to the considerable amount of time involved, the researcher had the opportunity to observe and participate in a variety of activities over time. Through these activities, the researcher was able to engage with the 10 members of Company A who were able to outline what the study meant to them as individuals and how they could use the findings to improve their current development process. Trust was an essential component in building relationships to get participants to open up (Taylor & Bogdan, 1984; Merriam, 1998; DeWalt & DeWalt, 2002; Wolcott, 2001; Lincoln & Guba, 1994)Several activities (DeWalt & DeWalt, 2002). Other best practices, including ethics, were considered to minimise researcher bias and maximise the efficiency of the field experience (Angrosino & dePerez, 2000).

4.9. Evaluation of the Field Notes and Writing up of the Results

To ensure accurate mapping, the researcher's biases were set aside (Kutsche, 1998). The mapping method was based on the approach of Kutsche (1998). The researcher created a detailed physical map of Company A's surroundings, using as much detail as possible. The company was studied several times to evaluate how the findings and recommendations were used in different application development projects. In order to practice cultural relativism, the researcher refrained from making value judgements and instead used relevant adjectives to meaningfully describe the different aspects of the environment (Schensul et al., 1999). Only one of the five senses, vision, is used in this mapping procedure. This observation phase was conducted from May 2020 and concluded in September 2020.

Table 15 summarizes the positive feedback, and the summarised constructs underpinning the insights acquired by Company A can be identified and integrated into the context of this research through the following constructs:

- A clearly defined and focused application security strategy;
- Strict alignment between the application security strategy and the organisation;
- A thorough consideration of the business and organisational context.

Table 15. Summary of the Results Achieved

Issue	Method	Source of Evidence
Improved the costs associated with application security training.	Interview	IDR_SE1
Improved the level of knowledge in the area of application security development.	Interview	IDR_SD
Improved awareness and eliminated any misperceptions with the developer team.	Interview	IDR_JD
Observed staff's understanding and commitment to application security best practices to dispel misconceptions.	Participatory observation	Researcher
Improved management willingness to invest in developing all developers.	Participatory observation	Researcher
Observe the behavior of stakeholders and employees.	Direct observation	Researcher

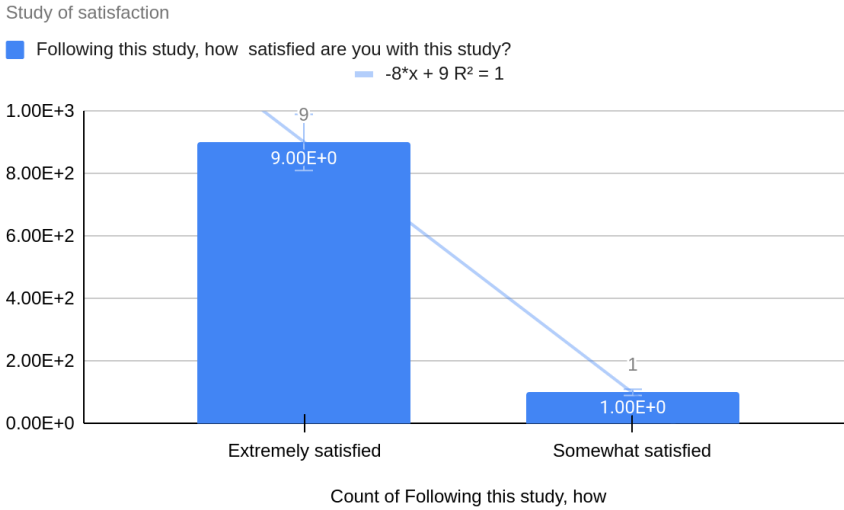


Figure 12. Participants and observers' satisfaction.

The satisfaction scale is depicted in Figure 12. The considerable drop is due to one participant's dissatisfaction with the security training, which focused on developers and application users but not on the whole organisation, including management and stakeholders. From a safety perspective, it is critical for companies to ensure that safety training is provided regularly to the entire company and not just to a select group. This should also be measured by the effectiveness of safety training, monitoring of

safety

incidents, feedback from employees, monitoring of changes in employee behaviour and attendance at training, all in line with the company's strategic objectives.

5.0. Threat to Validity (Limitations)

The data in this paper comes from two organisations and therefore the results of this study cannot be replicated by other researchers as the dataset is not publicly available. A data policy agreement was signed; which stated that the data collected would be utilized only for this study and would not be imparted to any third party. As the study was limited to two CRM systems, the results obtained may be specific to them, even though the applications used were from different organisations. There is also a possibility that the results would have been different if a wider range of applications, including commercial and open source applications, or even other application programmes developed in different languages, had been used.

This study was limited to Germany and in particular to software developers and IT security experts. However, since all employees play an important role in the security chain as they come into contact with the final product, the results could have been different if all these characteristics had been taken into account by analysing human interaction with the application and their security awareness training practices (e.g. phishing email campaigns).

Another limitation arose from the limited sample size. While it was sufficient to produce acceptable results, it would have been interesting to find out whether the hypotheses would have had the same validity in other sectors where business applications are developed by third parties by extending the study to external partners. Also, little attention was paid to the importance of the relationship between software developers' skills and management. Indeed, it would have been interesting to analyse the relationship between software developers, management and employee performance.

In addition, this type of validation is very time-consuming due to the large amount of data. Using six different hackers was relatively expensive and time-consuming.

The knowledge base in this work was built by uncovering each piece of the puzzle, and the limitations show where further efforts need to be made to improve this research. For example, the sample size should be increased or the same work should be applied to other sectors.

6.0. Implication

The main objective of this paper was to understand how compliance with an industry standard strategically impacts enterprise application security. The underlying assumption is that the increase in data leaks in the presence of an industry standard (e.g. ISO) can be mitigated by combining it with application development security best practices. A practical challenge, of course, is to foster this kind of awareness in enough cases to have a measurable positive impact on information security. The premise of this work is that by better understanding the interrelationships between human, technological and individual behaviour, commitment and attitude in relation to an organisation's security policy, the application of security best practices and any industry standards can be better configured and targeted to help organisations achieve their desired outcomes. Here, this study cannot conclude that compliance with an industry standard does not add value to the security of enterprise applications, but it can conclude that compliance alone does not convey security.

7.0. Conclusion & Future Work

Compliance with industrial standards does not convey application security. According to the findings of this study, organizations that rely on standards to increase application security fail to discover or detect possible threats in their applications. This is exacerbated by the fact that the majority of standard checklists fail to address data security or the secure data transfer mechanism. The vast majority of standards are centered on the information technology-driven process. A specific security assessment method is required for effective security engineering and integration into application programs, which is discovered in this study. This research uses software vulnerability prediction tools, Student t-tests and other data mining approaches to detect vulnerabilities in two CRM systems. The detection strategies in this study were based on four classifiers. Many organizations rely on standards that ignore a huge number of insecure systems with different unsustainable vulnerabilities and applications, which is ironic

yet compelling. The current scale of the cyber threat requires a security development approach that prioritises both application security and long-term viability. Furthermore, today's digitisation process requires various advanced requirements and utilities that are not provided by today's regulatory standards. In today's world, ensuring data integrity of sensitive applications requires more security policies and practices than just adhering to a standard. To support this idea, it is important that organisations that are compliant with the standard still develop a policy or framework for application security by focusing on the security factor of the ontology-based approach.

The future work of this study will encompass fifty distinct sectors with various application programs, their network, web application firewall settings, and their workers in terms of security policy compliance

according to categorization criteria in order to filter vulnerable requests. Having analysed some of the features of other CRM applications from other industries, this study can state with greater confidence that compliance with a standard alone does not convey security. It is therefore crucial to choose the right security concept to ensure a secure network and data transmission in applications to prevent cyber attacks. Assessing the vulnerability of cyber security systems and vulnerabilities to cyber attacks should be an essential activity. In conclusion, this study will be of great use to software project management, practitioners, freelancers and security experts to ensure that security is effectively and thoroughly considered in application development projects.

REFERENCES

- Agrawal, A., Alenezi, M., Kumar, R., Khan, R.A. (2019), "Measuring the Sustainable-Security of Web Applications through a Fuzzy-Based Integrated Approach of AHP and TOPSIS", *IEEE Access* 2019;7:153936–51.
- Agrawal, A., Alenezi, M., Kumar, R., Khan, RA. A. (2020), "unified fuzzy-based symmetrical multi-criteria decision-making method for evaluating sustainable-security of web applications", *Symmetry* 2020;12(3):448.
- Ahola, J., Fröhwhirth, C., Kutvonen, L., Helenius, M., Nyberg, T., Pietikainen, A., Pietikainen, P., Rönning, J., Ruohomaa, S., Sars, C., Siiskonen, T., Vähä-Sipilä, A., Ylimannela, V. (2014), "Handbook of the Secure Agile Software Development Life Cycle", University of Oulu, Finland.

- Ahola, J., Frühwirth, C., Kutvonen, L., Helenius, M., Nyberg, T., Pietikäinen, A., Pietikäinen, P., Röning, J., Ruohomaa, S., Särs, C., Siiskonen, T., Vähä-Sipilä, A., Ylimannela, V. (2014), "Handbook of the Secure Agile Software Development Life Cycle", University of Oulu, Finland (2014).
- Al-Ahmad, W and Bassil, M. (2013), "Addressing information security risks by adopting standards", *International Journal of Information Security Science*,2(2):28_43.
- Al-Khater, W. A., Al-Maadeed, S., Ahmed, A., Sadiq, A. S., and Khan, M. K. (2020), "Comprehensive review of cybercrime detection techniques," *IEEE Access*, vol. 8, pp. 137293–137311.
- Al-Matari, O. M., Helal, I. M., Mazen, S. A., and Elhennawy, S. (2020), "Integrated framework for cybersecurity auditing," *Information Security Journal: A Global Perspective*, vol. 29, pp. 1–16, 2020.
- Alenezi, M. and Khellah, F. (2015), "Evolution impact on architecture stability in open-source projects", *International Journal of Cloud Applications and Computing (IJCAC)*, 5(4):24–35.
- Ali, B. M., & Younes, B. (2013), "The Impact of Information Systems on User Performance", An Exploratory Study.
- Anderson, H. L. (1986), "Metropolis, Monte Carlo and the MANIAC", *Los Alamos Science*, vol. 14, pp.96–108.
- Angrosino, M.V., & dePerez, M.K.A. (2000)," Rethinking observation: From method to context", In Norman K. Denzin & Yvonna S. Lincoln (Eds.), *Handbook of Qualitative Research* (second edition, pp.673-702), Thousand Oaks, CA: Sage.
- Babak, A., Ashkan, T., Konstantinos, D. (2015), "Cloud Computing, Sustainability, and Risk: Case Study: A Quantitative Fuzzy Optimization Model for Determining Cloud Inexperienced Risks' Appetite", *sciencedirect* - <https://doi.org/10.1016/B978-0-12-801379-3.00015-2>.
- Baca, D. (2012), "Developing Secure Software -in an Agile Process", Doctoral Dissertation. Blekinge Institute of Technology.
- Baca, D. (2012), "Developing Secure Software in an Agile Process", Doctoral Dissertation. Blekinge Institute of Technology.
- Baca, D., Boldt, M., Carlsson, B., Jacobsson, A. (2015),"A novel security-enhanced agile software development process applied in an industrial setting. In: Proc. of ARES.

- Baca, D., Carlsson, B. (2011), "Agile development with security engineering activities", In: Proc. of ICSSP. pp. 149–158. ACM.
- Bárány, Imre, and Vu, Van. (2007), "Central limit theorems for Gaussian polytopes". *Annals of Probability*, Institute of Mathematical Statistics, vol. 35, no. 4, pp. 1593–1621.
- Bartsch, S. (2011), "Practitioners' perspectives on security in agile development", In: ARES (2011)
- Baskerville, R. (1999). *Investigating Information Systems with Action Research*. *Communications of the Association for Information Systems*, 2, pp-pp. <https://doi.org/10.17705/1CAIS.00219>
- Beck, K., Beedle, M., van Bennekum, A., Cockburn, A., Cunningham, W., Fowler, M., Grenning, J., Highsmith, J., Hunt, A., Jeffries, R., Kern, J., Marick, B., Martin, R., Mellor, S., Schwaber, K., Sutherland, J., Thomas, D. (2001)," Manifesto for agile software development".
- Bell, L., Brunton-Spall, M., Smith, R., Bird, J. (2017), "Agile Application Security. Enabling Security in a Continuous Delivery Pipeline", O'Reilly.
- Bell, L., Brunton-Spall, M., Smith, R., Bird, J. (2017),"Agile Application Security. Enabling Security in a Continuous Delivery Pipeline", O'Reilly.
- Beznosov, K., Kruchten, P. (2004), "Towards agile security assurance. In: Proc. of NSPW. ACM. Beznosov, K., Kruchten, P. (2004), "Towards agile security assurance", In: Proc. of NSPW. ACM.
- Bin, Y., Zhou, K., Lu, H., Zhou, Y., Xu, B. (2017), "Training data selection for cross-project defection prediction: which approach is better?", In: *International symposium on empirical software engineering and measurement*. IEEE Computer Society, pp 354–363.
- Bishop, M. (2005), "Introduction to computer security", Addison-Wesley Boston, MA.
- Calero, C. & Piattini, M.(2019),"Puzzling out software sustainability", *Sustainable Comput Inf Syst* 2019;16:117–24.
- Calero, C., & Piattini, M. (2015)," Introduction to green in software engineering", In: *Green in Software Engineering*. Cham: Springer; 2015. p. 3–27.
- Calero, C., García-Rodríguez De Guzmán, I., Moraga, M.A., García, F. (2019)," Is software sustainability considered in the CSR of software industry?", *Int J Sustain Dev World Ecol* 2019;26(5):439–59.

- Calero, C., Moraga, M., Bertoa, M.F (2013), "Towards a software product sustainability model. Sustainable Software for Science: Practice and Experiences; 2013. p. 1– 4. arXiv preprint arXiv:1309.1640.
- Carlson, T., Tipton, HF., & Krause, K. (2008), "Understanding Information Security Management Systems", Auerbach Publications Boca Raton, FL.
- Ch'oliz, J., Vilas, J., Moreira, J. (2015), "Independent security testing on agile software development: A case study in a software company", In: Proc. of ARES.
- Chowdhury, I. and Zulkernine, M. (2011). Using complexity, coupling, and cohesion metrics as early indicators of vulnerabilities. *Journal of Systems Architecture*, 57(3):294–313.
- D'Agostino, R., and Pearson, E. (1973), "Tests for departures from normality. Empirical results for the distribution of b_1 and b_2 ", *Biometrika*, vol, 60, pp. 613–622.
- Damiani, E., Ardagna, C. A., and El Ioini, N. (2008). *Open source systems security certification* Springer Science & Business Media.
- DeWalt, K.M. & DeWalt, B.R. (2002), "Participant observation: a guide for fieldworkers", Walnut Creek, CA: AltaMira Press.
- Duan T, Xiang J, Zhang H, Li Q-M. Research on simulation method of industrial control system attack based on hybrid tests. *Cyber Secur.* 2019;3:8–22. Search in Google Scholar
- Felderer, M., Pekaric, I. (2017), "Research challenges in empowering agile teams with security knowledge based on public and private information sources", In: Proc. of SecSe.
- Felderer, M., Pekaric, I. (2017), "Research challenges in empowering agile teams with security knowledge based on public and private information sources", In: Proc. of SecSe.
- Felderer, M., Pekaric, I.: Research challenges in empowering agile teams with security knowledge based on public and private information sources. In: Proc. of SecSe (2017)
- Fitzgerald, B., Stol, K.J., O'Sullivan, R., O'Brien, D. (2013), "Scaling agile methods to regulated environments", An industry case study. In: Proc. of ICSE. IEEE.
- Fitzgerald, B., Stol, K.J., O'Sullivan, R., O'Brien, D.: Scaling agile methods to regulated environments: An industry case study. In: Proc. of ICSE. IEEE (2013).

- Fitzgerald, B., Stol, K.J.: Continuous software engineering: A roadmap and agenda. In: *The Journal of Systems and Software*. vol. 123, pp. 176–189 (01 2017)
- Fitzgerald, B., Stol, K.J.: Continuous software engineering: A roadmap and agenda. In: *The Journal of Systems and Software*. vol. 123, pp. 176–189 (2017)
- He P, He Y, Yu L, Li B (2018) An improved method for cross-project defect prediction by simplifying training data. *Math Probl Eng* 2018:1–18. <https://doi.org/10.1155/2018/2650415>
- Herbold S, Trautsch A, Grabowski J (2018) A comparative study to benchmark cross-project defect prediction approaches. *IEEE Trans Softw Eng* 44:811–833. <https://doi.org/10.1109/TSE.2017.2724538>
- Hoffmann, R., Kiedrowicz, M., Stanik, J. (2016), "Evaluation of information safety as an element of improving the organisation's safety management", *MATEC Web of Conferences*, vol. 76.
- Hosseini S, Turhan B, Mantyl M (2016) Search based training data selection for cross project defect prediction. In: *ACM international conference proceeding series*. Association for Computing Machinery, New York, New York, USA, pp 1–10
- IEC: 62443-1-1 Security for industrial and automation control systems Part 1-1 Models and Concepts. USA, 2014 edn. (2014)
- Ifinedo, P. (2014), "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition", *Information & Management*, 51(1), 69-79.
- ISO/IEC (2013). *ISO/IEC 27002 – Information technology – Security techniques – Information security management systems – Requirements*. International Organisation for Standardization/International Electrotechnical Commission.
- ISO/IEC 27005:2018 *Information technology – Security techniques – Information security risk management– 2018*. [Online]. <https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en> [Accessed 6 September. 2021].
- ISO/IEC. (2017) "62443-4-1 Security for industrial automation and control systems Part 4-1 Product security development life-cycle requirements".
- Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, 32, 489-496.

Kali.org. (2014). SlowHTTPTest. [online] Available at: <https://tools.kali.org/stress-testing/slowhttpstest>.

Kawata, K., Amasaki, S., Yokogawa, T. (2015), "Improving relevancy filter methods for cross-project defect prediction", In: Proceedings—3rd international conference on applied computing and information technology and 2nd international conference on computational science and intelligence, ACIT-CSI 2015. pp 2–7

Kumar, D., Sharma, A., Kumar, R., Sharma, N. (2019), "Restoration of the network for next generation (5G) optical communication network", In 2019 International Conference on Signal Processing and Communication (ICSC). IEEE; 2019. pp. 64–8. Search in Google Scholar.

Kumar, R., Khan, S.A., Khan, R.A., (2015), "Revisiting software security risks". J Adv Math Comput Sci 2015:1–10.

Kutsche, P. (1998), "Field ethnography: a manual for doing cultural anthropology", Upper Saddle River, NJ: Prentice Hall.

Li, G., Zhou, H., Feng, B., Li, G., Li, T., Xu, Q., Quan, W. (2017), " Fuzzy theory based security service chaining for sustainable mobile-edge computing. Mobile Inf Syst 2017:1–14.

Lincoln, Y.S., & Guba, E.G. (1985), "Naturalistic inquiry", Beverly Hills, CA: Sage.

Luo, T., Hao, H., Du, W., Wang, Y and Yin, H (2011), "Attacks on webview in the android system", In Proceedings of the 27th Annual Computer Security Applications Conference, ACSAC '11, pages 343–352, New York, NY, USA, ACM.

Luthra, S., Kumar, S., Garg, D., Haleem, A. (2015)," Barriers to renewable/sustainable energy technologies adoption", Indian perspective. Renew Sustain Energy Rev 2015;41:762–76.

Mardani, A., Jusoh, A., Zavadskas, E., Cavallaro, F., Khalifah, Z. (2015),"Sustainable and renewable energy: An overview of the application of multiple criteria decision making techniques and approaches", Sustainability 2015;7 (10):13947–84.

Merriam, S.B. (1998), "Qualitative research and case study applications in education", San Francisco: Jossey-Bass Publishers.

McGraw, G. (2006), "Software security: building security in", volume 1. Addison-Wesley Professional.

- Medeiros, I., Neves, N. F., and Correia, M. (2014), "Automatic detection and correction of web application vulnerabilities using data mining to predict false positives", In Proceedings of the 23rd international conference on World wide web, pages 63–74. ACM.
- Moyón, F., Beckers, K., Klepper, S., Lachberger, P., Bruegge, B. (2018), "Towards continuous security compliance in agile software development at scale",. In: Proc. of RCoSE. ACM.
- Moyón, F., Beckers, K., Klepper, S., Lachberger, P., Bruegge, B.(2018), "Towards continuous security compliance in agile software development at scale", In: Proc. of RCoSE. ACM (2018).
- Nguyen, H.Q.(2001)," Testing applications on the Web: Test planning for Internet-based systems", John Wiley & Sons; 2001.
- Nyanchama, M. (2005), "Enterprise vulnerability management and its role in information security management", Information Systems Security, 14(3):29– 56.
- O'Mahony, M. (1986), "Sensory Evaluation of Food: Statistical Methods and Procedures", CRC Press, p. 487.
- Owasp.org. (2019). XSS Filter Evasion Cheat Sheet - OWASP. [online] Available at:https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet [Accessed 6 September. 2021].
- Owasp.org. (2018). cross-siteScripting(XSS)-OWASP.[online]Available at: [https://www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)) [Accessed 6 September. 2021].
- Oyedeji, S., Seffah, A., Penzenstadler, B. A. (2018)," catalogue supporting software sustainability design", Sustainability" 2018;10(7):2296.
- Pavlov, G., & Karakaneva, T. (2011), "Information security management system in organisation", Trakia Journal ofSciences, 9(4):20_25.
- Penzenstadler, B., Raturi, A., Richardson, D., Tomlinson, B.(2014), " Safety, security, now sustainability", The nonfunctional requirement for the 21st century. IEEE Softw 2014;31(3):40–7.
- Powers, David M. W. (2011), "Evaluation: From Precision, Recall and F-Measure to ROC, Informedness, Markedness & Correlation". Journal of Machine Learning Technologies. 2 (1): 37–63.

- Safa, N. S., Von Solms, R., & Furnell, S. (2016), "Information security policy compliance model in organisations", *Computers & Security*, 56, pp. 70-82.
- Sahu, K., Rajshree, Kumar, R.(2014)," Risk management perspective in SDLC", *International J Adv Res Comput Sci Softw Eng*. 2014:1247–51.
- Sahu, R.K. (2019)," Srivastava Revisiting software reliability Data management, analytics and innovation", Springer Singapore 221 235.
- Schensul, S.L., Schensul, J.J., & LeCompte, M.D. (1999)," Essential ethnographic methods: observations, interviews, and questionnaires (Book 2 in Ethnographer's Toolkit)", Walnut Creek, CA: AltaMira Press.
- Schieferdecker I. Responsible Software Engineering. In: *The Future of Software Quality Assurance*. Cham: Springer; 2020. p. 137–46.
- Scarfone, S., Souppaya, M., Cody, A. & Orebaugh, A. (2008), "NIST SP 800-115, Technical Guide to Information Security Testing and Assessment", Gaithersburg, MD, USA: National Institute of Standards and Technology.
- Siponen, M., Baskerville, R., Kuivalainen, T. (2005)," Integrating security into agile development methods", In: *Proc. of HICSS*.
- Siponen, M., Baskerville, R., Kuivalainen, T. (2005),"Integrating security into agile development methods", In: *Proc. of HICSS*.
- Stallings, W., Brown, L., Bauer, M.D., Bhattacharjee, A.K. (2012), "Computer security: principles and practice (pp. 978–0)", Upper Saddle River. NJ: Pearson Education.
- Stallings, W., Brown, L., Bauer, M.D., Bhattacharjee, A.K., (2012)," Computer security: principles and practice", (pp. 978–0). Upper Saddle River. NJ: Pearson Education.
- Stephanow, P., Khajehmoogahi, K. (2017),"Towards continuous security certification of software-as-a-service applications using web application testing techniques", In: *Proc. of CAINA*.
- Stewart, H. (2020), "Information Technology and Cyber Security Unplugged": The interrelationshipbetween Human Technology and Cyber Crime Today (English Edition), Rohhat LTD" 2020.

- Stewart, H. (2021), "The hindrance of cloud computing acceptance within the financial sectors in Germany", *Information and Computer Security*, Vol. ahead-of-print No. ahead-of-print.
<https://doi.org/10.1108/ICS-01-2021-0002>
- Stewart, H., and Jürjens, J. (2017), "Information security management and the human aspect in organisations", *Information & Computer Security*, vol. 25, no. 5, pp. 494–534.
<https://doi.org/10.1108/ICS-07-2016-0054>.
- Stewart, H., and Jürjens, J. (2018), "Data security and consumer trust in FinTech innovation in Germany", *Information & Computer Security*, vol. 26, no. 1, pp. 109–128.
<https://doi.org/10.1108/ICS-06-2017-0039>.
- Taylor, S.J., & Bogdan, R. (1984), "Introduction to qualitative research: The search for meanings", (second edition), New York: John Wiley.
- Tøndel, I.A., Jaatun, M.G., Cruzes, D.S., Moe, N.B. (2017), "Risk centric activities in secure software development in public organisations. *IJSSE* 8(4), 1–30.
- Tøndel, I.A., Jaatun, M.G., Cruzes, D.S., Moe, N.B. (2017), "Risk centric activities in secure software development in public organisations", *IJSSE* 8(4), 1–30.
- Tounsi, W. and Rais, H. (2018), "A survey on technical threat intelligence in the age of sophisticated cyber- attacks," *Computers & Security*, vol. 72, no. 3, pp. 212–233.
- Tufan, E., Tezcan, C., and Acartürk, C. (2021), "Anomaly-based intrusion detection by machine learning: A case study on probing attacks to an institutional network," *IEEE Access*, vol. 9, pp. 50078–50092.
- Turpe, S., Poller, A. (2017), "Managing security work in scrum: Tensions and challenges", In: *Proc. of SecSE*
- Upadhyay, D. and Sampalli, S. (2020), "SCADA (supervisory control and data Acquisition) systems: Vulnerability assessment and security recommendations," *Computers & Security*, vol. 89, no. 3, pp. 101666.
- Vaca, A. J. V., Gasca, R. M., Fombella, J. A. C. and Lopez, M. T. G. (2020), "AMADEUS: Towards the AutoMAteD secUrity testing," in *Proc. of the 24th ACM Conf. on Systems and Software Product Line: Volume A-Volume A*, New York, NY, United States, pp. 1–12.

Venters, C.C., Capilla, R., Betz, S., Penzenstadler, B., Crick, T., Crouch, S., Carrillo, C. (2018), "Software sustainability: Research and practice from a software architecture viewpoint", *J Syst Softw* 2018;138:174–88.

Walden, J., Doyle, M., Lenhof, R., and Murray, J. (2010), "Idea: java vs. php: security implications of language choice for web applications", In *Engineering Secure Software and Systems*, pages 61–69. Springer.

Wolcott, H.F. (2001), "The art of fieldwork", Walnut Creek, CA: AltaMira Press.

Zhang, S., Caragea, D., and Ou, X. (2011), "An empirical study on using the national vulnerability database to predict software vulnerabilities", In *Database and Expert Systems Applications*, pages 217–231. Springer.

Zhou, D. (2020), "Research on the security strategy and technology of information resource network of chinese academy library", *J Phys Conf Ser.* 2020;1550:032037.

Conclusion to STUDY 3: Security versus compliance: an empirical study of the impact of industry standards compliance on application security

Study 3 examined the inability of industry standards to prevent the current sophisticated cyber threats to digital transformation services and products. The results of this study made it clear that security and compliance are a necessary part of any sector. However, inadequate security of digital products and services was seen as the main barrier to the adoption of digital transformation technologies, as also noted in studies 1 and 2. The study also points out that although security received more attention than compliance with industry standards, it is important to understand how both impact data security.

Digital transformation companies rely heavily on the trust of their customers, and a security breach can damage their reputation. On the other hand, adherence to and certification of an industry standard strengthens trust between business partners, as they can be confident that they are adhering to a standard rather than the necessary security. Security measures are driven by financial risks, while compliance is driven by legal obligations and shows business partners that a company can be trusted to protect their data from threats. .

As a result, security and compliance can be viewed as two distinct parts of a crucial and essential system. Given that each element depends on the other to maintain the greatest level of data security, it is essential to understand how they relate to data protection in the context of digital transformation.

Study 3 thus confirms the research questions identified in Chapter 1 on the influence of security and trust on the use of digital products and services. However, given the uncertainty of the challenges of digital transformation, the question arises as to which current gaps in the IS/IT strategy literature contribute to the greatest challenges for companies in digital transformation regarding security and which elements contribute most effectively and successfully to the security of a company's digital transformation. Therefore study 4 aims to explore and explicate the challenges and elements that are the key attributes to enhance digital transformation security. Study 4 is presented in the next chapter.

Chapter 7. STUDY 4: Digital transformation security challenges

Introduction

The fourth study is an extension of studies 1, 2 and 3 and looks at the security challenges of digital transformation, which remains one of the biggest challenges for managers. As Study 3 found that compliance with an industry standard alone does not provide assurance in digital transformation, it is crucial to explore what indicators can be used to determine the quality-of-service assurance and make decisions. Therefore, Study 4 delves into the elements that can be addressed by managers to gain a complete view of emerging risks and apply certainty in rapid experiments.

By measuring the cue congruency effect and the impact of various elements, Study 4 aims to examine the interaction between managers and various elements and their influence on improving security. In the face of ongoing international cyberattacks, management is focusing on cybersecurity. IT staff are no longer the only ones who should be concerned. To prevent the crippling effects of data breaches, rapid, sophisticated attacks across all industries have shown that cybersecurity is the responsibility of the entire organisation.

It is also important to note that technology and traditional security strategies are not scalable as they are not able to protect the current converging transitions, as humans play an important role in technology. Therefore, convergent innovation requires convergent security and to achieve this, the pace of security transformation must match that of digital transformation. To achieve effective security throughout the lifecycle, security must be integrated into all facets of digital technology. This security transformation also encompasses the entire distributed ecosystem, which includes human resilience to cyberattacks, identifying the attack surface, defending against known threats, detecting threats, responding quickly and effectively to cyber incidents and conducting ongoing assessments.

Organisations tend to be sceptical about digital transformation and their acceptance. The adoption of these innovative decisions is influenced by their perception of cybersecurity. It could be argued that organisations' perceptions of the legitimacy of security solutions influence their expectations of service quality and purchase intentions. However, existing research contains relatively few findings on the elements that need to be considered to develop a mature cybersecurity strategy. Study 4 fills these

gaps by identifying and analysing elements that are typical impediments to digital innovation in organisations by addressing common elements that influence digital transformation security through a literature review and a case study.

The paper is authored by Harrison Stewart with contributions corresponding to the contribution ratio for this article, which is set out on the next page.

<https://doi.org/10.1080/08874417.2022.2115953>

Statement of Authorship

CO-AUTHORSHIP APPROVALS FOR HDR THESIS EXAMINATION

PUBLICATION 4

This section is to be completed by the student and co-authors. If there are more than four co-authors (student plus 3 others), only the three co-authors with the most significant contributions are required to sign below.

Please note: A copy of this page will be provided to the Examiners.

Full Publication Details

Digital Transformation Security Challenges

Harrison Stewart (2022) Digital Transformation Security Challenges, Journal of Computer Information Systems, DOI: 10.1080/08874417.2022.2115953

Section of thesis where publication is referred to

All

Student's contribution to the publication

<u>100</u>	%	Research design
<u>100</u>	%	Data collection and analysis
<u>100</u>	%	Writing and editing

Outline your (the student's) contribution to the publication:

Harrison Stewart is the sole owner of this publication.

APPROVALS

By signing the section below, you confirm that the details above are an accurate record of the students contribution to the work.

Name of Co-Author 1 _____ Signed _____ Date _____

Name of Co-Author 2 _____ Signed _____ Date _____

STUDY 4

Digital Transformation Security Challenges

Harrison Stewart

Abstract

Digital transformation has become one of the most popular strategies for information systems (IS). Developing and implementing a digital strategy is a mandatory task for any organization that relies on information systems. In this digital age, an IS/IT strategy without security considerations could lead to serious data breaches. Despite all countermeasures, security remains a major concern in digital transformation, as digitization is misjudged and brings with it major security concerns. The digitization of manual goods, processes and services, as well as their use, leads to various security issues in different organizations. The aim of this study is to identify and analyze elements that are typical barriers to digital innovation in organizations. This study addresses common elements that impact the security of digital transformation through a literature review and a case study.

Keywords – Digital strategy security, Digital Strategy, Digital Transformation, IS/IT Strategy security, information security, digital security

Paper type - Research paper

1.0. Introduction

Digitalisation has impacted research on IS/IT strategy development, and several studies on IS/IT strategies have been conducted in the literature, providing various solutions, insights and frameworks that are relevant and useful for practitioners and academics (Arbanas & Hrustek, 2019). Considering the digital age and the high number of cybercrime incidents, several studies have urged organisations to incorporate security into their digital strategy (Lundgren & Möller, 2017). Factors like confidentiality, integrity and non-repudiation, are all fundamental elements in digital transformation security. The term "integrity" refers to the assurance that a communication or transaction has not been tampered with. Non-repudiation establishes the existence of a communication or transaction and assures that its contents cannot be challenged after it has been transmitted (Lundgren & Möller, 2017; Collet, 2020; Karpunina et al., 2019; Stewart & Jürjens, 2018). Digital strategy encompasses both the technical and human activities within an organisation and describes how the lifecycle of an organisation's digital strategy practices should be managed. Academics and practitioners have long been concerned about the security of digital strategies, and a survey conducted by the digital association found that cyber-attacks cost over US \$103 billion in 2018/2019, rising to 10.5 trillion US\$ by 2025 (Sausalito, 2020), highlighting the impact of cybersecurity on businesses as a whole. These issues show that companies need to recognise and address digital security as a strategic issue, not just an IT issue. In the past, risk management in traditional IS/IT strategy was based on cost structure and higher value, which is different from today's IS/IT strategy where cybersecurity has become a strategic investment in information and communication technology (ICT) and a prerequisite for a company's long-term sustainability. As a result, there remains a disconnect between risk management efforts and the development of key cybersecurity capabilities. Therefore, a critical assessment of the current state of the art in terms of academic initiatives and practitioner perspectives is required.

Over the years, a substantial body of academic research has been built in the area of digital innovation, and some research has addressed the security of digitisation and the information it contains (Duc & Chirumamilla, 2019; Ande et al., 2020). Research on malware, phishing, password attacks and social engineering attacks on information systems has evolved over the decades (Eder-Neuhauser et al., 2018; Bullée & Junger, 2020; Hadnagy, 2018). The attackers' goal is to spy on, modify, delete and gain unauthorised access to data, resulting in significant financial and reputational damage (Sausalito, 2020; Oliveira et al., 2017; Stewart & Jürjens, 2017). Several organisations are attacked every day, either knowingly or unknowingly (Hu & Wang, 2018; Burda et al., 2020).

In 2021, there was a staggering 105 per cent increase in ransomware cyberattacks worldwide. These attacks aim to harm individuals or businesses by rendering their computer systems inoperable until they pay a ransom (Thorwat, 2018; Arbanas & Hrustek, 2019). According to the Cyber Threat Report 2022, released Thursday by cybersecurity firm SonicWall, ransomware attacks increased 1,885 percent globally in 2021, with the healthcare industry seeing a 755 percent increase. In North America, the number of ransomware attacks increased by 104 percent, which is only slightly below the global average of 105 percent. Although academic study on security in general has been done, the focus has tended to concentrate on security policy, phishing security, and computer security which have all been studied in different ways.

This study is crucial for achieving a balance within the establishment of sufficient controls and the ever-changing nature of cyber attacks. Thus the study is guided by the following research questions;

- RQ1; What are the current gaps in past literature on IS/IT strategy that contribute to the biggest challenges for companies in digital transformation when it comes to security?
- RQ2; What are the elements that are most effective and successful in contributing to the security of a company's digital transformation?

To establish definitive proof and prevent bias, a topic selection criterion must be undertaken based on the selected research topics. Once the main research phase is completed, this paper adopted Pan and Tomlison's research guidelines (2016). The references on the main search phase's selected articles are extensively checked, and if the paper fulfils relevant criteria, it will be included in the synthesis. Furthermore, a financial company is used as a case study for analysing the concept of security in digital strategy to provide conceptual clarity. The basic definition of information security according to Stewart

(2022) states that information systems security is about maintaining the integrity of the logical and formal components of information systems. Consequently, information security refers to the protection of data, process and information. Similar concepts of information systems and security can also be found in other literature (Samonas & Coss 2014, Luse et al. 2013). All subsequent literature evaluations in IS security research have been limited to specific streams of study (e.g., compliance) within the field, rather than broad assessments of the field's trajectory.

The paper begins with an introduction in Section 1, then explores the characteristics of organisational IS security in Section 2, and finally provides an overview of different IS security theories in Section 3. Section 4 of this paper discusses the case study of a financial institution on the security challenges of digital transformation, while Section 5 discusses the research methodology before presenting the results in Section 6. Section 7 discusses the findings and Section 8 concludes with an analysis of the common elements impacting IS security. In conclusion, the scope of this research is confined to the security of digitization (Baskerville, 1993; Siponen, 2005).

2.0. Literature Review

There are numerous studies in the literature by various researchers on factors affecting information systems security (Alhogail et al., 2015; Alhogail et al., 2014; Allam, Flowerday, & Flowerday, 2014; Arbanas & Hrustek, 2019). Al-Omari et al., (2012) focus on user compliance with ICT regulations to investigate the factors that influence the security of information systems. Al-Hogail (2015) examines security culture as a factor in maintaining an organisation's information systems. Stewart (2022) proposes a framework that addresses the development and implementation of information security policies (ISPs), while Alhogail, Mirza & Bakry (2015) proposed a framework that addresses only the human aspects of IS protection.

Dillion (2021) conducts a systematic review of the literature on information systems security by performing topic modelling of the major information systems journals to understand the debate in the field; conducts a Delphi study with senior information security executives of major companies in the US to identify the security issues they consider important; and compares the results of the topic modelling and the Delphi study; and discusses the major controversies, gaps and paradoxes found in the scientific literature. Dillion then addresses the lack of synergy between academic research and practical concerns and proposes a future research agenda in three broad themes, namely: IS security design; attacks; vulnerabilities; compliance and behaviour.

Baskerville (1993) published the first literature review on IS security as a model made up of three eras that are linear in time and advance. Each of these eras has its own set of tactics, as well as goals, means, obstacles, and philosophical assumptions that distinguish them from one another. The first era, which originated in the early 1970s with the purpose of mapping constrained solutions to an information issue, is referred to by Baskerville as checklist techniques. This era's security was achieved by the use of checklists and risk assessments, and was mainly based on product supplier documentation.

The third era of Baskerville builds on logical transformation methods and consists of a highly abstracted design that describes the problem and solution space. Structured analytical data modelling and entity-relationship diagrams are common development methods and tools for this era, while logical control designs and data flow diagrams are common security tools.

Baskerville (1993) suggests three distinct security risks based on his overview. First, Baskerville claims that IS security management uses a mechanical approach to complexity partitioning. Second, there is a focus on the bare minimum of controls required to meet protection standards. Third, there is a dualism of growth. According to Baskerville, security is treated as an add-on to the overall architecture of information systems. Instead, he believes that the architecture of information systems should incorporate all aspects of security from the outset.

Siponen (2005) asserts in a review that, while researchers have established various new methodologies, old approaches like checklists, standards, maturity criteria, risk management, and formal procedures continue to dominate research.

Security is still treated as an outcast by system designers due to competing priorities between security goals and information use (Stewart, 2021; Stewart, 2022); White and Dhillon (2005) define duality in secure systems development as the process by which "an information system and its security are designed, built, and implemented separately in an organisational environment, allowing for the possibility of conflict between a system's functionality and its security" (Albrechtsen 2007). Such dualism is defined by Spagnoletti and Resca (2008) as 'drift,' which happens when the technological system deviates from the initial plan. Evidence of development dualism, as initially conceived by Baskerville, predominates, as evidenced by various research (Paananen et al., 2020).

Future IS security research should include social and organisational elements, according to Dhillon and Backhouse (2001). The human and behavioural components are subsumed under the social and

organisational variables (Stewart & Jürjens, 2018). McFadzean et al. (2006), Siponen (2005), and Siponen and Oinas-Kukkonen (2005) all emphasised the need of incorporating similar aspects in later years (2007). Many other academics have noted the underlying organisational issues, especially when it comes to policy compliance (Stewart, 2022; Karjalainen et al. 2019).

Other theories have been explored recently by researchers in their attempt to discover answers to problems affecting the security of information systems (Zoto et al., 2018; Shahri & Mohanna, 2016; Han, Dai, Tianlin Han, & Dai, 2015; Lubua & Pretorius, 2019; Stewart, 2022). Recognizing diverse IS security concepts and their achievements aids in analysing the IS security literature and identifying elements that impact an organisation's IS security. Socio-technical theory, distributive cognitive theory, general deterrence theory and the Nine-Five-Circle (NFC) (Stewart & Jürjens, 2017) theory are the most often used IS security theories.

2.1. Security Theories for Information Systems

2.1.0. Socio Technical Theory

The concept of bringing together and considering both "socio" and "technical" components as interrelated pieces of a complex system underpins social-technical theory. Organisations that concentrate on a single aspect of the system fail to analyse and comprehend the system's deep linkages. The role of the human factors in IS security has been considered in this theory as an important factor in detecting and preventing data breaches. This has been studied by many researchers, and Stewart (2017) pointed out that human factors play an important role in cybersecurity. Although many consider cybersecurity as a technological factor, socio technical theory remains an effective approach for designing system security and its environment through the analysis of goals, culture, technology, humans, infrastructure, process, procedure. usability challenges, internal security governance, and security needs (Zoto et al., 2018; Charitoudi & Blyth, 2013). As a result, socio technical theory is applicable to explore ways in which humans contribute to an organisation's IS security based on their perceptions and approach to IS security.

2.1.1. Distributed Cognitive Theory

Distributed cognition, developed by Edwin Hutchins, is the belief that information exists not just inside an individual, but also within the individual's social and physical surroundings. The idea focuses on self-efficient processes by focusing on how a person may use skills rather than what kinds of abilities they have, hence it can be applied to information system security as security self-efficacy (Shahri & Mohanna, 2016). As information is spread more in a virtual environment, the idea recommends collaboration among individuals to achieve common goals. As a result, information system security should be associated with human cognition (Han et al., 2015).

2.1.2. General Deterrence Theory

The goal of general deterrence is to prevent illegal behaviour. To discourage is to deter. According to the concept, humans would avoid committing crimes because they are afraid of the harsh repercussions. This idea was used for information system security with the goal of inducing dread of repercussions in individuals to deter them from taking actions that might jeopardise the system's security (Hu et al., 2011). As a theory based on certainty and gravity of consequences, it proposes a range of measures/punishments to be implemented depending on the gravity of a given person's illicit actions contrary to information security. This idea is particularly important in IS security because of the high prevalence of cybercrime and its financial consequences (Lubua & Pretorius, 2019).

2.1.3. Nine-Five-Circle (NFC) Theory

By considering the security culture of the organisation, the NFC integrates the three theories to prevent criminal behaviour, improve human behaviour, and improve the design and security of information systems. The theory focuses more on measuring and evaluating the IS security performance of organisations and improving the link between technology, process and human factors (Stewart & Jürjens, 2017; Stewart, 2021; Stewart, 2022).

Despite the efforts of many researchers to propose various ideas that could be effective in protecting the security of information systems, the theories have failed to identify the true causes of the problems before attempting to solve them, which this study attempts to do.

Therefore, the NFC seems to be more relevant because it incorporates all three theories and other aspects into one theory as detailed in all the aforementioned theories. To identify and comprehend the fundamental origin of an IS security breach in an organisation, a case study is used in this study.

3.0. Case Study

The study serves to illustrate the key features of a financial institution's digital strategy implementation programme and how it can help explain constructs of success and key events in IS security (Doukidis et al., 2020). Due to the nature of the company, it was deemed necessary to make greater use of staff knowledge and experience to help the company prevent data breaches that could damage its reputation (Collet, 2020; Duc & Chirumamilla, 2019; Stewart & Jürjens, 2018). The company in this study operates in the banking sector and has made the strategic decision to use digitalisation to create new value, increase transparency, embrace a robo-advisor, reduce costs, increase convenience, improve approval rates, increase efficiency and security, and provide consumers with better access to information (Hess et al., 2016; Legner et al., 2017; Stewart & Jürjens, 2018). The company has three directors and 5 board members. It has been operating for 30 years. It has 15 branches in Germany, spread over 10 sub-regions, and employs more than 1200 humans. The company has a large share of the German market and is considered one of the most innovative financial sectors today. The company is supervised by the Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), the financial supervisory authority in Germany.

To achieve this digitalisation goal, the management has set up a dedicated digital department with a team of software engineers to implement a digital transformation to the market (Singh & Hess, 2017; Stewart, 2022). As a result, more than 300 employees have started their duties in the digital department, contributing to the success of the sector. This digital department adheres to the organisation's numerous standards and centralised IS/IT strategy; yet, the transition to digitalisation requires a different approach than the traditional IS/IT strategy. Although, the number of security threats has risen as a result of the organisation's fast digital transformation (Singh & Hess, 2017; Stewart, 2022). Their existing strategy, as depicted in Figure 1, fails to handle contemporary security risks, causing significant impediments in the digital transformation.

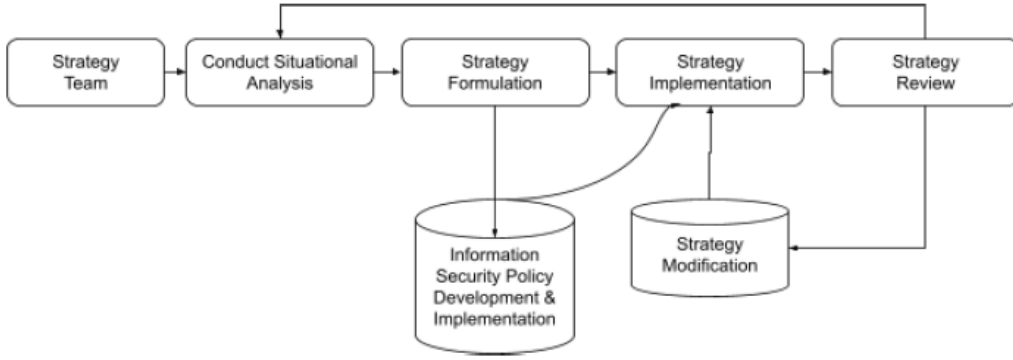


Figure. 1 The organisation’s current IS strategy and Digital Strategy

Table 1. Contemporary cyber risks classification

	Intentional & Unintentional		
Incident Consequence	External party	Internal party	Risk Impact
DoS/DDoS	A disruption at a third-party provider disrupts the firm.	An act disrupts the firm's operations.	High
Data Breach - PII	A third-party provider employee uses physical access to steal PII classified data from the firm.	A firm employee uses physical access to steal PII data from the firm.	High
Theft or Loss of Non PII Information	A third-party steal non-PII firm data from a third-party provider via remote access.	With remote access, an external party steals non-PII firm data.	Medium
Theft of Funds	An external party defrauds the firm, causing financial loss to the firm or its customers.	An employee of the firm uses their access to steal money from the firm or its customers.	High

3.1. Problem Identification

Based on the information collected during the assessment phase in section 3, it was clarified that data breaches and high funds are among the challenges that the organisation encounters as shown in Table 1. The cost of the most recent data breach, according to management, was estimated at \$4.01 million, with an average data breach of 12 records each year. On the other hand, these episodes have shattered the trust of consumers and partners, forcing investors and customers to cease conducting business with the company (Gordon et al., 2011).

To gain the trust of consumers and investors and drive digital transformation, the company must have appropriate IS security measures in place to protect itself from cyber attacks and insider threats while delivering secure services and goods. Understanding IS security qualities is critical for determining which security key elements are important during digital transformation. Organisations pursuing digital transformation must go beyond the traditional ISO27001 security definition of Confidentiality, Integrity, and Availability (CIA) security baselines and qualities, which has been the core emphasis of any information security strategy (Stewart, 2022). Despite the fact that this CIA has become the industry standard, the organisation in this study fails to recognize these IS security attributes, and thus fails to protect or has inadequate protection, resulting in an increase in IS security breaches, which will have a significant negative impact on their digital transformation (ITU, 2017; Fields et al., 2016).

4.0. Research Methodology

The contribution of this paper is twofold: first, it follows a literature review/secondary study and assesses the security of digital transformation in an organisation. For this purpose, three public and available well-known databases and search engines, namely Google, Wikipedia and Google scholar, were consulted and a case study to support this work. A survey was conducted in the organisation in this paper, followed by a pilot test, interviews and data analysis (Duan et al., 2019; Zhou 2020; Kumar et al., 2019; Walsham 2006). The results are validated using an observational approach (Baskerville, 1999), system evaluation techniques and a feedback technique.

4.1. Content Analysis

This study uses the topic modelling approach to find important hidden topics in the emerging IS security academic literature. The search was limited to abstracts, titles and author keywords of articles published in information management journals with an academic journal guide ranking of A or higher between January 2014 and January 2021. To limit the search engine's capacity to discover the document and to limit fine search, special characters such as ("/", "-", "(", ")") were employed. The result was 4298 articles, with a final sample size of 2938 due to some abstracts that were irrelevant to the study. The focus of the 2938 articles was on the security of information systems in the context of digital transformation processes (Huang et al. 2018). Mainstream topics like information security, work environment and demographic factors are ignored in this study.

To remove redundant or noisy material, the collected abstracts were screened for errors by removing certain expressions such as "the, the, a, are" and performing word normalisation. The LDA approach is used to model the abstracts of these articles and uncover latent themes (Blei et al., 2003). The ideal number of subjects is estimated using two reduction algorithms proposed by Cao et al. (2009) and Arun et al. (2010), and two maximisation techniques proposed by Griffiths and Steyvers (2004) and Deveaud et al. (2014).

Similar to the work of Mahfuth et al. (2017), a research checklist is created to ensure that the data extraction process meets the requirements. The work of Hassan et al. guides the quality of data extraction (2015). This study's checklist employs three scales, each of which is categorised and assigned a score. The final score is calculated by adding the sums of the individual elements on the checklist. The scale runs from 0.5 to 5, with 5 being the highest possible score.

4.2. Discussion of Content Analysis Findings

Table 1 indicates the synthesis's quality rating based on the quality evaluation. The quality ranking of all key research publications is shown in Table 2. Low-quality studies were disregarded because they lacked particular findings or research techniques. Finally, the ideal number of subjects was set at 39, which were then extracted using LDA in the R topic models package.

Table 2. Topic analysis

Exploration Type	Scores
------------------	--------

Quantitative	61%
Qualitative	12%
Formal experiments	9%
Mixed Techs	10%
Case study	1% (as indicated in this study)

4.3. Data Collection

The primary source of data for this study was a survey conducted to confirm and complement the results of this study. A questionnaire was developed and distributed to 40 security experts, managers, stakeholders and all executives. The overall objectives of the survey, resources, budget and timeframe were determined by the management and researchers in line with best practices in questionnaire development (Umbach, 2004). By mutual agreement between the researchers and the management, the survey was conducted through an internet survey, a postal survey, a telephone interview and a face-to-face interview (Bishop et al., 1998; Witmer et al., 1999; Walsham 2006). These methods were agreed upon by the researchers and management based on their advantages and disadvantages. The question format was then designed to include both open and closed questions (Neuman, 2007). The survey also contained closed-ended Likert scale questions that required respondents to select from a list of prepared answers. The flow of questions was then designed to create a logical sequence of questions by rejecting responses from unqualified respondents (Sax et al., 2003), ensuring that respondents felt comfortable and provided honest information (Myers and Newman 2007; Walsham 2006). The surveys were organised into five sections: (a) introduction; (b) answer pre-screening; (c) welcome questions; (d) progression to more detailed and challenging questions; and (e) conclusion. The questionnaires were evaluated on whether they were required, how lengthy they were, and whether they contained all the information required for this study. The researcher pre-tested the questionnaire and, after approval by the client, made changes that resulted in the final layout of the questionnaire, which the client accepted.

The questionnaire received 40 responses from experts who are involved in the organisation's IS strategies and have a great influence on the development of their IS strategy. For the data analysis, SPSS was used. Although the pilot test included 65 questions in the initial phase, only 25 questions were included in the final questionnaire based on feedback from the pilot test. The interviews lasted 45

minutes. Semi-structured interviews were then conducted to gain a deeper understanding of employees' perceptions and opinions of their current digital strategy, particularly in relation to current cyber threats and their ability to secure their innovative ideas. As in the work of Britten (1995), open-ended questionnaires were used to conduct the interviews, starting with simple questions and progressing to more complex and sensitive topics. The data collection phase was conducted with direct participation from staff, the IS strategy department and the IT security department.

The adaptation of the questionnaire contributed to obtaining a clear understanding of the organisation in the case study digital transformation processes. For the selection of respondents, a systematic sample technique was adopted (see Table 2). In this instance, the researcher chose every n th person,

$$\text{where } n = \frac{200}{20} = 10 \quad (1)$$

There were 200 employees in total, divided by ten, giving a total number of two. Every second person was selected here. As a result, the sample size was reduced to 20 participants who were identified anonymously to maintain anonymity (Walsham, 2006), as indicated in Table 3.

Table 3. Employee Tags Used for Anonymity

Group of users	Number of users	Anonymous ID
Senior executives, CIO	2	IDR_01, IDR_02
Digital Strategy Manager	3	IDR_03
IT Decision Maker	3	IDR_04
Security Manager (CISO)	1	IDR_05
IT-Staff & Network	2	IDR_06, IDR_07
DevOPs	9	IDR_08, IDR_09, IDR_10

During the analysis phase, the interview data was categorised in order to identify any difficulties pertaining to variables impeding digital strategy security growth. These interviews were utilised to validate the content analysis codes in section 4.1 as well as the components employed in this study.

4.4. Factors Affecting Digital Transformation Security (DSS)

The study uncovered 39 studies on information security conducted in both the public and private sectors, as well as by individuals working in these domains. The goal was to figure out why digital security or IS security, is still an issue for most businesses (such as the case study in this article) and individual users of modern technology.

From the synthesis, the data analysis revealed 8 topic areas explored in mainstream IS security research, as described in the preceding section (see Table 3). The findings show that the most common themes in the sector are stakeholder and employee misconceptions about information security which is associated with individual behaviour and negligence. Individual behaviour and compliance are directly related to the components of some of the following information security myths (e.g. cyber security is not my responsibility; hackers do not target small businesses; phishing is not my concern; strong passwords protect me; we only need to protect ourselves against external hackers; inadequate data encryption; and simple antivirus software is enough to protect data). It is vital for organisations to raise employee awareness of cyber security by establishing processes to educate and train employees on such myths and their associated security threats to the organisation. This approach will help employees to adjust their behaviour and recognise their role in the cyber security chain and know what needs to be protected and why. Behavioural adjustments to increase security compliance or minimise breaches have been the subject of several research publications. Other findings include, threat and vulnerability assessment, organisation cyber security strategy, software engineers secure system engineering, security monitoring, advanced threat investigation strategy, and incident reporting and remediation strategy.

Stewart (2022) investigates the obstacles to successful information security initiatives, whereas other researchers focus on the effects of intrinsic behaviour that leads to non-compliance (Karjalainen et al., 2019; Dhillon et al., 2020) of information policies. It is therefore important that a high level of cyber security awareness and a strong security culture is developed within an organisation. Table 4 displays the findings of many research that reflect the eight constructs;

Table 4. Factors affecting the security of the information system or digital transformation

DSS Constructs		Definition
Security Misperception	SM	IS/IT Strategy and Digital Strategy Misconception
Evaluation of threat Vulnerability and Risk	ETVR	Threats, vulnerabilities, and mitigation techniques that are linked to the digital strategy and assist to reduce the overall risk.
Cybersecurity Strategy	CSS	Action plan to improve the security and resilience of electronic products and services. It is an overarching, top-down strategy for cybersecurity that sets out a series of goals and priorities to be achieved within a specific timeframe.
Secure System Engineering	SSE	Integration of secure software engineering tools, methodologies, and processes into the software life cycle.
Security Testing and Evaluation	ST&E	Analyse and assess the security measures required to secure digital services and goods. Reduces threats and risks in systems and lowers the likelihood of losses due to a cybersecurity breach.
Protective Monitoring	PM	Automatic security checks based on logs created by systems or applications.
Strategic Advanced Threat Intelligence	SATI	Strategic threat intelligence provides a comprehensive Overview of an organisation's threat landscape.
Incident Response and Remediation	IRR	Respond to incidents quickly and efficiently to maximise effectiveness.

5.0. Developing the Security in Digital Strategy

The study is divided into two sections. The first part of the study, which lasted from January 2020 to August 2021, included the research review and the case study in the organisation. The second phase, called the evaluation phase, started in September 2021 and ended in January 2022. In this phase, the eight factors and their implementation in the organisation are discussed. The participants' comments, observations and interviews are used to evaluate this study.

The eight constructs are discussed in more detail in this stage.

(I) Security Misperception

The role of security in digital transformation is highly misjudged by executives and IT decision-makers in various organisations (Collett, 2020; Karpunina et al., 2019). Stewart (2020) emphasised the importance of managers' perception of security and pointed out that the misperception of security among managers and employees is due to several factors that prevent organisations from developing a well-defined secure culture. In addition to Stewart, other research studies have also attempted to identify the various reasons for the varying degrees of challenge in developing digital security strategy. For example, managers' perceived conflict between security and usability (Andriotis et al., 2015; DeWitt et al., 2015). Stewart (2020) examined various academic literature and reports from information security institutions on the evolution of security and highlighted four factors that influence the misperception of security, namely: speed, usability, privacy and value (Stewart & Jürjens, 2018). Various organisations consider security at the expense of usability, which then leads to a major conflict between security and usability (Dhillon et al., 2016). According to Kraemer et al. (2009), organisational and human aspects are closely linked to information security, while Stewart (2020) emphasises how interaction between humans and technology can improve information security. Without user engagement, the development and implementation of DSS would be challenging, so user behaviour in the context of the digital security lifecycle is critical to success.

Apart from the misconceptions of the executives, there was also a huge misconception of secure coding among the software engineers (Mlitz, 2021) and the security teams (Duc & Chirumamilla 2019, Li et al., 2020) due to factors such as lack of security knowledge, lack of teamwork, budget constraints, lack of prioritisation of security, lack of commitment, security tools and culture, security controls to be implemented and their proper implementation. Considering the incentives between the security teams and the software development teams, both teams were encouraged to play on the same team to avoid disagreements by aligning their interests and creating complementary incentives. Several data breaches were the result of security failures that hindered the remediation of vulnerabilities in digital products and services (Stewart & Jürjens, 2018; Collett, 2020; Karpunina et al., 2019). Software engineers who refuse to adhere to an established security framework or security standards are also a major bottleneck in many organisations, as this leads to shadow IT. Stewart (2022) defines shadow IT as a means of misusing information systems, e.g., the unauthorised storage and processing of data. This phase allowed senior leaders and all stakeholders to see themselves as targets of cyber attacks, dispelling the myth that their organisation is worthless or uninteresting to cyber criminals. Their overconfidence in

security and the fact that they do not see themselves as a target, which in turn could create opportunities for hackers, were discussed. At this stage, the researcher and participants were able to develop a strategy that led the participants to think about cyber-physical attacks as well. They considered the physical impact an attack could have on their business and internet, which in turn could have an impact on their offices and staff. The main objective of this phase was to ensure that stakeholders supported this work with both budget and resources.

(II) Evaluation of threat Vulnerability and Risk

A cyber threat is defined as any harmful behaviour aimed at causing harm to cyberspace (anything connected to a computer): Cyber threats include data breaches, identity fraud, ransomware, data corruption, and so on. Once an attacker strives to infiltrate a system, they are attempting to undermine the system's confidentiality, integrity, and availability (CIA). These three concepts form the CIA triad, sometimes referred to as the AIC triad. Confidentiality preserves the privacy of the data or information, i.e. access to confidential data must be restricted to authorised persons. Integrity preserves the legitimacy and integrity of the data or information, i.e. both data and information must not be manipulated by an unauthorised user during transmission or storage. Availability refers to the accessibility of the service or data, i.e. authorised users should be able to access the services and data at any given time.

Digitisation requires a "security by design" approach that minimises vulnerable coding errors and vulnerabilities. To achieve this, software engineers were provided with security guidelines, including the Open Web Application Security Project's (OWASP) Top 10 White Paper, the Groupe Spéciale Mobile Association's (GSMA) "GSMA IoT Security Guidelines & Assessment", the IoT Security Foundation's "Secure Design Best Practice Guides" and the Cloud Security Alliance's "Future Proofing the Connected World: 13 Step to Developing Secure IoT Products".

(III) Cybersecurity Strategy

Due to the large volume of data they manage, the organisations in this study are perfect targets for cyber attackers (Collett, 2020; Stewart, 2021; Chooi & Ahmad, 2017). The lack of a security strategy

within the digital transformation strategy has contributed to their current vulnerability. This phase should identify what cybersecurity strategy is recommended and how comprehensive these studies are within the organisation. Although several researchers and practitioners have recommended their own security strategies, these recommendations cannot be applied to the organisation in this study, as observed by Stewart (2020). Meaning, the same security framework cannot be applied to multiple organisations due to different needs. Therefore, the researcher proposes his own strategy in this study by adapting key points from previous studies and neglecting industrial norms.

The purpose of the cybersecurity strategy in this study is to assure the CIA of the organisation's digital transformation, which has been accomplished by providing proactive, effective, and active assistance and development. As the cybersecurity strategy is an overall plan to ensure the security of digital transformation, it is crucial to regularly update the digital security strategy. Considering the importance of humans in cyber security strategy, establishing a rigid security culture is an essential factor in an organisation.

Although this study does not omit information security policies (Lucila, 2016; Flowerday and Tuyikeze 2016; Stewart, 2022), compliance (Sohrabi et al., 2016) and information security management (Flowerday and Tuyikeze 2016), cybersecurity requires a more proactive approach as opposed to a reactive approach (Soomro et al., 2016; Stewart & Jürjens, 2017). Organisations with various security requirements and objectives have different security requirements and objectives (Karyda et al. 2005; Ines 1994; Wood 2004). According to Baskerville and Siponen (2002), it is critical to understand the organisation's security requirements while designing security initiatives. As a result, the organisation should define its security objectives, including the level of security it aspires to attain. Here, the focus was on preventing cyber-attacks and incidents in advance. The company's cyber threat landscape situation was analysed by exploring the products and services developed and the types of cyber attacks to which they are exposed (Collett, 2020; Stewart, 2021). Next, the threats in the supply chain were analysed, e.g. compromised components used for the final products utilised by the company's customers and partners.

The advanced awareness of the threats facing the company enabled the researcher and participants to develop an effective cybersecurity strategy. During this phase, the threat attributes faced by the organisation were presented in a descriptive manner. The NIST cybersecurity framework was then used to assess the level of cybersecurity maturity. This assessment was divided into the following categories:

(i) policy, (ii) governance and (iii) incident recovery skills (Joshi et al., 2017; Stewart & Jürjens, 2017). The assessment covered traditional IT operations technology, the Internet of Things and systems.

As mentioned earlier, cybersecurity is a continuous process rather than a product (Stewart, 2021). As a result, the stated cybersecurity program was continually amended in order to meet the established strategic goals. The defined solutions were submitted to management for assessment, feedback, and approval. Management expressed its support since the misconception concerns were first handled (Stewart & Jürjens, 2017; Stewart, 2022). To meet the strategic objectives, the whole approach was extensively documented, including risk assessments, cybersecurity plans, policies, guidelines, and procedures. Individual duties were clearly stated and feedback was obtained from participants. Cybersecurity awareness and training efforts were also conducted (Stewart & Jürjens, 2017; Karumbaiah et al., 2016).

(IV) Secure System Engineering

Software engineering is critical to digital transformation (Mlitz, 2021; Stewart, 2022), which brings with it a number of challenges, such as cyber threats which could lead to organisational financial loss (Collett, 2020; Stewart, 2021). According to a study by Duc & Chirumamilla (2019), attackers often look for vulnerabilities in software designs and architectures to gain access to a person's or company's information. Stewart (2022) concluded in his study that compliance is not synonymous with security and that companies relying on industry standards to improve digital security need to develop an application security strategy rather than relying on an industry standard.. Based on this study, the software development team was able to identify the important security factors that need to be considered at all stages to create effective and resilient software that can withstand all security attacks (Li, 2020; Stewart, 2020). In addition to software security, additional measures were taken to prevent threats such as malware, denial-of-service attacks and hacking (Doukidis et al., 2020).

The researcher, including the CISO and security strategy facilitators, explained to the executives the importance of storing, processing and transmitting consumer data, leading the executives to identify significant threats to their digital transformation strategy posed by insecure software. Management was advised to give software security the highest priority and to invest in improving software security measures (e.g. through training and seminars on software security)(Collett, 2020). The organisation's digital transformation can be protected from the threats of data leaks, data breaches and financial theft by integrating security into the digital strategy (Stewart & Jürjens, 2017; Stewart & Jürjens, 2018). At

the end of this phase, the managers recognised the need to allocate sufficient resources to ensure that software was developed with security in mind to prevent intrusion by attackers. This phase emphasised the importance of software security for rapid and effective digital transformation in the organisation.

(V) Security Testing and Evaluation

Risk assessment includes a component called security test and evaluation (ST&E). To test and improve the security of software, vulnerability detection and security assurance through security testing are usually used at this point. Implementing appropriate security testing procedures has become a critical step in conducting effective and efficient security testing, so this stage of testing was crucial. This phase was also concerned with developing refined approaches and applying and disseminating them in practice (Bertolino et al., 2014; Ayewah et al., 2008; Acker et al., 2012; Appelt et al., 2014).

The researcher at this stage focused on three groups that contribute to digital transformation, namely humans, processes and products, all of which contribute to system security. As Stewart & Jürjens (2017) states, the NFC addresses the interrelationships between these three groups and provides a solution to the problem. In this study, the human aspect consists of the software engineers, staff and IT managers (Stewart & Jürjens, 2017), the process consists of manual and automated procedures (Acker et al., 2012), while the product is represented by the digital product or service (Stewart & Jürjens, 2018). In general, the same security challenges are common to all, but each group faces its own challenges when it comes to continuously complying with the established security rules.

a. Humans:

Due to the various challenges, cyber security training and awareness measures have been implemented, including a strict security policy required for compliance at all stages of the product life cycle.

b. Process (Technology):

According to Stewart (2022), developmental security testing/evaluation encompasses the entire system development lifecycle, including all post-design phases. This phase demonstrates that the required security controls have been implemented correctly, are operating as expected, security policies have been enforced appropriately, and comply with established cybersecurity standards. Any inclusion of vulnerable components from suppliers or changes to these components may impact the

security posture of the final product and the security controls currently implemented in this study (Bertolino et al., 2014; Appelt et al., 2014). Therefore, it is critical to establish rigid control levels to allow software engineers to perform additional security testing/assessment to reduce or eliminate uncertainties. When testing custom software applications, Stewart (2022) recommends static analysis, dynamic analysis, binary analysis or a mixture of these three approaches, which can be performed during code review or using different tools (e.g. binary analysers and application scanners) (Ayewah et al., 2008).

The researcher, together with the security team, developed security assessment rules and procedures that were followed by the engineers (Stewart, 2022). These plans specified the types of analyses, tests, evaluations and reviews that should be performed for software and firmware components, the level of rigour and the artefacts produced during these processes (Bertolino et al., 2014; Ayewah et al., 2008; Acker et al., 2012; Appelt et al., 2014). Stewart's (2022) definition of security testing/evaluation refers to the severity and complexity of the evaluation process (e.g. black-box, grey-box or white-box testing), as shown in Figure 2. The coverage of security testing/evaluation refers to the scope (i.e. quantity and type) of artefacts included in the evaluation process.

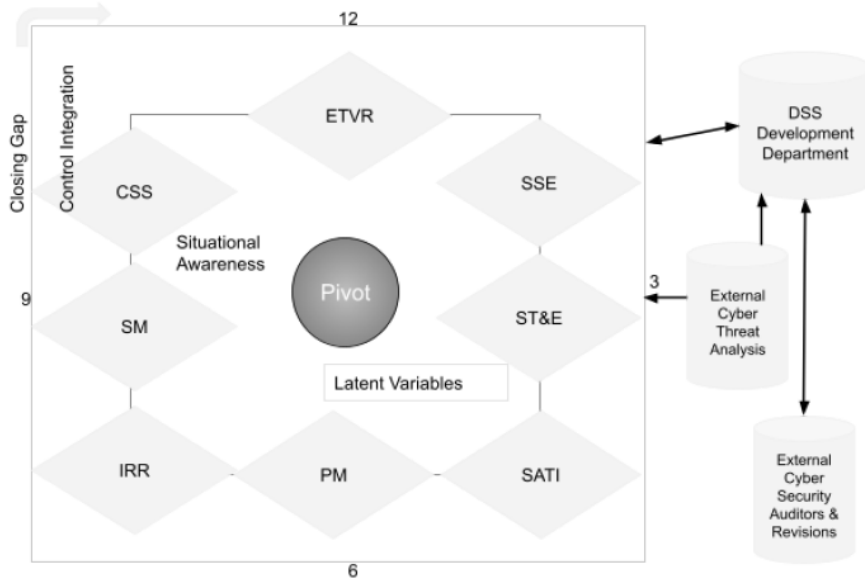


Figure 2. Digital transformation security framework consisting of all 8 constructs, latent variables and other components.

(VI) Protective Monitoring

In this study, more vulnerabilities, e.g. related to human error, their software products and systems, were uncovered through proactive monitoring (Moeini et al., 2019; Da Veiga & Martins, 2015). This technique involved security inspections and audits conducted by the security review team and facilitators. The aim of this monitoring was to obtain performance feedback that enabled corrective action to be taken before failures occurred in the development and implementation of the digital security strategy.

Thus, in order to achieve this effectively, the researcher set up a risk assessment team led by a competent person to assess the existing work practices based on the proposed NFC methodology and organisational systems (Luo et al., 2019). Their main role was to be proactive by conducting work-specific risk assessments, analysing the level of implementation of the proposed framework, reviewing the adequacy of the implementation of the digital strategy, and overseeing the overall cybersecurity management system through monitoring and audits (see Figure 9) (Luo et al., 2019).

Furthermore, a system was set up to establish ground rules that would be followed by all employees and comply with legal obligations. According to the researcher, the importance of this step was to analyse the financial and operational aspects of the organisation and to identify and assess vulnerabilities. Since security is not a product but a continuous process, this study conducted proactive monitoring at regular intervals to determine what needs to be updated and what needs to be fixed. The main objective of this proactive monitoring was aimed at developing a concept for the security and sustainability of digital products and services (Stewart & Jürjens, 2018).

This approach contributes to maintaining digital security and improving the security performance of digital transformation (Stewart & Jürjens, 2018; Collett, 2020; Karpunina et al., 2019).

This phase allowed the researcher to assess the extent to which the security strategy guidelines proposed in this study were followed. The involvement of managers was crucial in this phase as they were to ensure that their involvement promoted good performance (Terlav et al., 2016).

(VII) Strategic Advanced Threat Intelligence

Threat intelligence has been neglected in the development of a digital strategy. According to Stewart (2020), threat intelligence is a critical construct in the development of security strategies. Incorporating threat intelligence issues into the digital security strategy or IS/IT security strategy can help organisations identify vulnerabilities during the development lifecycle. It also improves security awareness among employees. When engineers know which vulnerabilities to improve during the development lifecycle, they become aware and can identify where a hacker might make a request or attack the product and services. Improving threat intelligence can alert both engineers and staff of malicious attempts. These alerts may also enable them to take the appropriate action and report incidents to the security department. In reference to Padayachee (2012), the intelligence value of threats obtained by an organisation is defined as the difference between the direct and indirect benefits of specific knowledge about their threats. Thus, the threat information derived in this study was documented and distributed to both software engineers and the entire organisation (Stewart, 2022).

In conclusion, a strategic threat intelligence system was established by the researchers and participants to direct the digital transformation department. Stewart (2020) recommends that staff in the critical data department receive regular security training to strengthen their cybersecurity skills and ensure that all digital department staff participate in cyber defence. All members of the digital department were keen to learn more at this stage. They were aware of the importance of cyber security as well as its advantages.

(VIII) Incident Response and Remediation

This section develops effective handling of security-related incidents, covering technical, cultural and organisational aspects. Recent reports show an increasing number of cybersecurity incidents resulting in significant financial losses (WEF, 2019). Despite the fact that the organisation in this study has a specific cybersecurity budget, incidents continue to occur. The linear incident response system depicted in Figure 3 is used in this study to prevent, identify, mitigate, remediate, and educate on cybersecurity incidents.

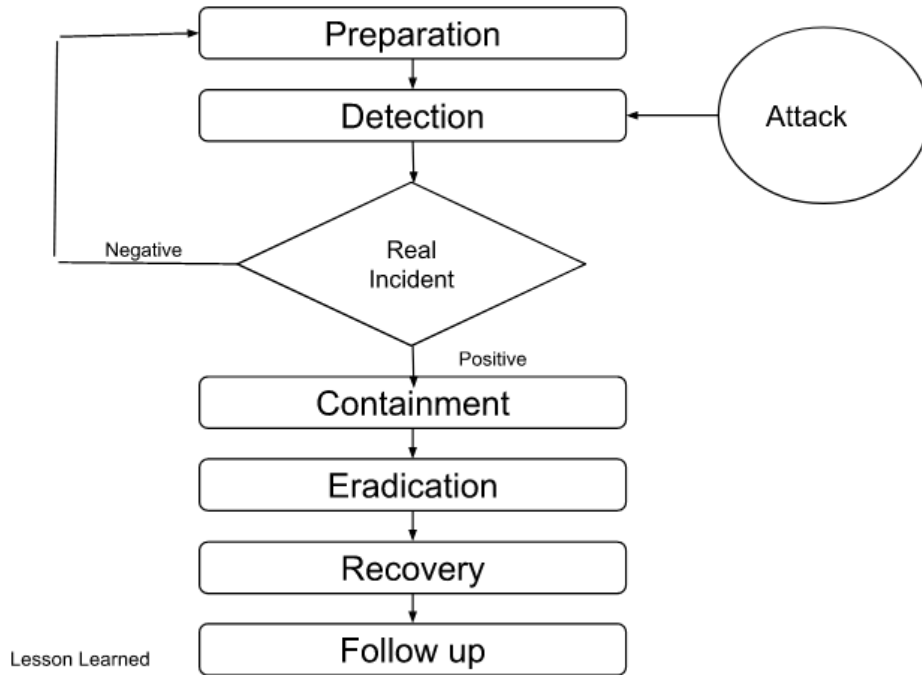


Figure 3. Linear incident response framework

Due to the complexity and persistence of their cyber threats, a specialised cyber security incident response team was critical to the security strategy proposed in this study (Morgeson et al., 1997; Ahmad et al., 2012). This team involves members from the IT department, legal department, corporate communications, human resources and other departments. A contingency plan (e.g. based on NIST Special Publication 800-61 Revision 2) is then provided to the team as a basis for managing such situations from early detection to recovery. Five key persons were then selected to manage the incidents, conduct the incident investigation, analyse the scale of the incident, determine the role of crisis communication and make leadership decisions (Helsloot & Groenendaal, 2011).

The team was trained on how to handle security incidents, covering everything from detection to reporting, which led to a standardised protocol for reporting cybersecurity issues across the organisation. To aid in identifying and mapping possible intrusions, incident response teams were given a suite of software tools that allowed them to scan network traffic records and visualise information flow. The training phase improved the team's cyber situational awareness to gain advanced knowledge of their systems and network activities, which also helped to conduct a continuous risk assessment (Ahmad et al., 2021).

This stage of the research gave the incident response team the capacity to prevent and identify incidents in the first place, as well as the technological capability to respond to cybersecurity incidents (Ahmad et al., 2020).

6.0. Observations and writing up of the Results

The observation is based on a systematic strategy in which greater emphasis was placed on specific actions in order to emphasise the differences in this study (Angrosino & dePerez, 2000). Due to the obvious length of the period, the researcher was able to observe and participate in a range of activities over a longer period of time. As a result, 20 members of the digital department were able to define the impact of the study on their daily activities and how the findings could improve their existing process for developing security strategies.

A basic framework was used to assemble the digital teams in this study, defining 16 core tasks or competencies that are essential for the creation and maintenance of most digital objects. In the end, three conceptual teams were formed to address these tasks: the digital business team, the digital technology team and the extended business team.

The digital business team defines the key business measures and objectives as well as the user interface/user experience (UI/UX). The digital technology team sets front end coding standards and chooses frameworks for any applicable technology. They are in charge of the system and quality assurance. The extended business team aims to create partnerships and campaigns to drive traffic.

To improve collaboration and foster relationships, certain roles and procedures were established. Building relationships requires trust for individuals to open up. Other good practices, such as ethics, have been explored to reduce researcher bias and increase the efficiency of the field experience.

Before analysing the eight constructs of the elements of success or failure, a basic question needs to be answered. *When and how can it be determined whether a digital strategy security program is a success or a failure?* The assessment procedure was conducted methodically to determine the answer to the question as shown in section 4.3. The overall findings were reassuring as listed in table 5.

Table 5. Summary of the Results Achieved During the first phase

Participant Groups	Interviewee
--------------------	-------------

#1	<i>Interviewee #IDR_01 and #IDR_02 noted that cybersecurity knowledge growth has increased over time, while #IDR_04 noted the positive change in executive attitudes and behaviours towards cybersecurity strategy, and #IDR_05 saw that the misconception of security is also a key construct for the organisation's strategic goals."</i>
#2	<i>Interviewee #IDR_05 specifically pointed out that this study has provided criteria and benchmarks for good security architectures and solutions, as well as methods to achieve them. Better mechanisms to hide and/or manage complexity were also cited by #IDR_06, while #IDR_04 noted that their previous incident response processes lacked flexibility. Respondent #IDR_03 mentioned that prior to this study, most of their systems were not creating event logs, which was a barrier to incident detection.</i>
#3	<i>Interviewees #ID_08, #IDR_09, IDR_10 and IDR_06 pointed out that the availability of capable staff has always been a major obstacle to an effective data security strategy, but this study has removed that obstacle.</i>
#4	<i>The two researchers in this study (#RS01 and #RS02) pointed out the importance of monitoring employees' understanding and commitment to cyber security.</i>
#5	<i>Researcher #RS02 also addressed the issue of increasing investment in cybersecurity projects.</i>
#6	<i>Both the #EA01 and #EA02 auditors had the task of auditing stakeholders and staff.</i>

In summary, the structures underpinning organisational outcomes may be recognized and understood within the proposed framework and are characterised by the following constructs:

- a coherent and well-defined DSS;
- maintain close coherence between the DSS and the organisation;
- an appropriate focus on all the different dimensions of digital strategy and security;
- a thorough assessment of the organisational and corporate landscape.

Table 6. Summary of the Results Achieved During the first phase

Issue	Method	Source of Evidence
Improve the costs associated with the security programmes of the digital strategy.	Interview	IDR_01
Improve the level of knowledge in the field of digital transformation security.	Interview	IDR_04
Improved awareness and elimination of misperceptions.	Interview	IDR_02, IDR_03, IDR_04, IDR_05, IDR_06, IDR_09, IDR_10
Improved digital transformation strategy aligned with corporate security.	Interview	Senior Executive
Monitor staff understanding and commitment to "Secure by Design" to eliminate misunderstandings.	Participatory observation	2 Researchers (RS01, RS02)
Improved management willingness to invest in cybersecurity projects.	Participatory observation	2 Researchers (RS01, RS02)
Examine the actions of stakeholders and staff.	Direct Observation	2 External Auditors (EA01, EA02)

Despite the beneficial results listed in Table 6, there were still some issues that this research tackles in order to remedy some of the organisation's inadequacies.

- c. Assessing the security programme for the digital strategy is a controversial and sensitive issue that needs to be addressed. This is crucial for the long-term sustainability of the digital transformation project and the implementation of the budgeting process, which is also necessary for the full recognition of the security function of the digital strategy in the company.

- d. In addition, the digital strategy security programme should continue to involve the entire organisational pipeline. The DSS framework has been kept simple in terms of design: Digital security strategy is about human compliance with defined policies, not about computer capability.
- e. The simplicity and ease of use of the DSS framework is an important attribute that helps in developing the security programme for the digital strategy within the organisation and for other organisations. However, more specific and complex technologies are likely to be critical.

The three bullet points have been addressed accordingly. A continuous update and improvement of the digital strategy was conducted to address the open points (a) and (b), while the third point was addressed by reiterating the NFC life cycle during a change that affects the current established strategy.

The recommended strategy improved the company's digital sovereignty and consequently its digital transformation, which in turn, strengthened the company's digital economy. A security-by-design strategy was a critical component of this study and one of the key technological enablers. The strategic framework recommended in this paper sets out the organisation's cybersecurity policy, which is divided into key principles, scopes of action and set of strategic targets.

7.0. Success Factors

The eight constructs were coded using the Vivo coding method. This technique is a type of qualitative data analysis that focuses on the respondents' actual words. In other words, it enables text coding using terms and expressions from qualitative data. Question 2 in this study, for example, can be classified as critical success factors because it refers to the success factors for cybersecurity implementation, which is where other subtopics are classified. This umbrella term encompasses subtopics such as awareness and training, security policies, compliance, and top management. Seminars, workshops, training, and other subtopics fall under the training and awareness subcategory. These subtopics combine to form a more abstract concept of training and awareness-raising, which can be abstracted further as one of the key success factors for successful cybersecurity implementation. The final coded themes from the qualitative data are shown in Table 7.

Table 7. Critical success factors for cybersecurity.

Critical Success Factors	Frequency	Percentage* (n=40)
--------------------------	-----------	--------------------

<i>Raising awareness, training and education</i>	23	57%
<i>Cybersecurity budget</i>	21	53%
<i>Security policy and compliance</i>	19	48%
<i>Senior management and stakeholders</i>	17	43%
<i>Application security</i>	16	40%
<i>Infrastructure security</i>	16	40%
<i>Communications and Collaboration</i>	11	46%
<i>Security professionals</i>	11	26%
<i>Audit of security</i>	7	18%
<i>Accountabilities for security</i>	3	8%
<i>Organisational structure</i>	1	3%

The goal of this phase was to identify and comprehend the necessary conditions for successful cybersecurity implementation, as cybersecurity challenges differ from organisation to organisation. Respondents were asked to name at least four critical success factors for cybersecurity in their organisation. The following are the top five cybersecurity success factors for the organisation in this study, according to Table 6 of the survey data:

- Awareness, training and education
- Security policy and compliance
- Cybersecurity budget
- Senior management and stakeholders
- Application security

According to the survey results, nearly 57% of respondents prioritised security awareness and training. 53% emphasised the importance of adequate budgets for cybersecurity projects, while 48 percent emphasised the importance of security policies and compliance. Furthermore, 43% of respondents mentioned senior management and stakeholders, while 40% mentioned application security and infrastructure security. These indicators contribute to a company's cybersecurity success factors and

provide an answer to the basic question raised in section 6: *“When and how can it be determined whether a digital strategy security program is a success or a failure?”*

8.0. Discussion

The study compares the major underlying assumptions to better understand the challenges of digital transformation in the context of traditional IT/IS strategy techniques. The misconception of digital strategy and IT/IS strategy was one of the major outcomes of this study. Security initiatives tend to be tackled by software engineers as an afterthought, so usability often takes precedence over security (Stewart, 2022). In subsequent years, other IS security initiatives have proposed several mainstream programmes, such as information security policy (Flowerday & Tuyikeze, 2016; Lucila, 2016), human behaviour and compliance (Furnell and Clarke, 2012; Crossler et al. 2013; Stewart, 2022).

Other literature evaluations, on the other hand, have encouraged academics to consider both digital transformation security and IS/IT security. The contributions of research to the eight security constructs in this work were examined from several angles. The technical, intellectual, and organisational levels of these eight constructs were all addressed. This study deals with the security of information systems from the perspective of digital security strategy.

9.0. Implications

In this study, a conceptual framework was developed to explain the influences on the development and outcomes of the digital strategy. The study considers past papers and a case study. This study has significant implications for practice. For example, the proposed framework with the eight constructs has the tendency to explain the influences on digital transformation and information security research findings. The framework provides a new perspective to study the evolution of an organisation's digital transformation and the development of secure digital strategy and some success factors. This work has justified the applicability of the proposed framework to elucidate the actions required in digital strategy projects by systematically testing the interrelationships between all eight constructs, thus answering the research question 2 as well.

This study has brought a new perspective to explain why digital transformation strategies require more than the traditional IS or IS/IT strategy process. Furthermore, the success of incorporating security into

IS/IT security or digital security requires the engagement of several factors that must work together to achieve a successful security strategy.

In practice, this study can serve as a reference for innovative organisations and their managers to set up a strategic security process by highlighting the context of digital strategy to enhance staff recognition, e.g. by providing them with security training to improve staff awareness. Other latent variables such as business strategy and business processes, while playing an important role in digital strategy, are not the main key to developing a secure digital strategy. Therefore, a secure digital strategy can be achieved by combining the eight constructs in this study, by arranging them in a structured way for an effective digital strategy security development and implementation.

10.0. Limitations

The study focused on a single financial organisation in Germany. The inclusion of survey participants from other organisations may have resulted in different perspectives and mindsets. Furthermore, including respondents who are not ICT professionals may have yielded different results. The survey results, on the other hand, provide a list of conceptual areas that could be further investigated to confirm their relevance to cybersecurity effectiveness. More empirical research is clearly required to validate the approach and the applicability of the observed success factors, as well as to improve its effectiveness. It would be extremely beneficial to extend it to other scenarios in the same sector for comparison and cross-analysis. It could also be applied to other industries where quite different aspects are the focus.

11.0. Conclusion

The research questions in this study contribute to the process of developing and implementing a secure digital strategy. Eight constructs were analysed and evaluated to create a model for developing a secure digital strategy. The research included a comprehensive examination of the current state of digital strategy security and the reasons for its success or failure. The synthesis of the literature is used to determine the most important/critical factors for IS security so that organisations do not make the wrong decisions. The study found that a misconception of security among various factors by leaders in an organisation, leading to ignorance of security among employees and affecting the culture of security, is seen as the main obstacle in embedding security in strategic digital transformation, which answers research question 2 (Parsons, McCormac, Butavicius, & Ferguson, 2010).

Apart from the importance of management involvement and employee acceptance of information security, the study also identified other factors such as threat vulnerability and risk assessment, which include threats, vulnerabilities and mitigation techniques that are linked to the digital strategy and help reduce overall risk. Cybersecurity strategy, which includes an action plan to improve the security and resilience of electronic products and services. It is an overarching, top-down cyber security strategy that sets out a series of objectives and priorities to be achieved within a specific time frame. Secure systems engineering, which involves the integration of secure software engineering tools, methods and processes into the software life cycle. Security auditing and assessment, which involves the analysis and evaluation of security measures required for the security of digital services and goods. The goal is to reduce threats and risks in systems and to reduce the likelihood of losses due to a cyber security breach. Protective monitoring, which includes automatic and manual security checks based on logs generated by systems or applications. Strategic advanced threat intelligence, which includes strategic threat intelligence to provide a comprehensive overview of the threat landscape of an organisation. Finally, there is the incident response and remediation factor, which includes proactive, rapid and efficient incident response to ensure maximum effectiveness. The important aspects to consider when creating and implementing a digital security plan in an organisation are addressed in this response to research question 1, which is part of the gaps in the previous literature on IS/IT strategy.

Insufficient understanding of these key factors for digital transformation security has led to a persistent risk to corporate information security. Furthermore, the factors identified in this study play an important role in security and form a common attribute, namely a combination of humans (knowledge, education and training), technology (secure programming and coding) and processing (continuous security training of employees and constant network monitoring). Therefore, the paper proposes the solution of using the NFC theory to ensure that other theories such as (social technical theory, distributed cognitive theory and general deterrence theory) are considered in information security initiatives.

The significance of raising awareness of the security of digital strategies is highlighted in this study, which will serve as an incentive to prioritise appropriate digital security and its communication to employees. This will act as an incentive to bridge the gap between the percentage of organisations that take security precautions and those that do not. When it comes to security, the challenges of digitisation for businesses undergoing digital transformation are numerous in Germany.

References

- Acker, S. V., Nikiforakis, N., Desmet, L., Joosen, W. & Piessens, F. (2012), "FlashOver:Automated discovery of cross-site scripting vulnerabilities in rich internet applications".
- Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organisational learning. *Journal of the Association for Information Science and Technology*, 71(8), 939-953.
- Ahmad, A., Hadjkiss, J., & Ruighaver, A.B. (2012), "Incident Response Teams - Challenges in Supporting the Organisational Security Function", *Computers & Security*. 31(5), (pp. 643–652).
- Ahmad, A., Maynard, S.B., Desouza, K.C., Kotsias, J., Whitty, M., & Baskerville, R.L., (2021), "How can Organisations Develop Situation Awareness for Incident Response? A Case Study of Management Practice", *Computers & Security*. Vol 101. (pp. 1-15)
- Al-Omari, A., El-Gayar, O., & Deokar, A. (2012), "Security Policy Compliance: User Acceptance Perspective", *IEEE*, 45(12), 1-10.
- Albrechtsen, E. (2007)," A Qualitative Study of Users, View on Information Security," *Computers & Security* 26 (4), 276–289.
- AlHogail, A. (2015)," Design and validation of information security culture framework", *Computers in Human Behavior*, 49, 567- 575.
- Alhogail, A., Mirza, A., & Bakry, S. H. (2015)," A comprehensive human factors framework for information security in organisations", *Journal of Theoretical and Applied Information Technology*, 78(2), 201-211.
- Alhogail, Areej; Mirza, A. (2014), "A framework of information security culture change", *Journal of Theoretical and Applied Information Technology*, 64(2), 540-549.
- Allam, S., Flowerday, S., & Flowerday, E. (2014), "Smartphone information security awareness, A victim of operational pressures" *Computers & Security*, 42, 56-65.
- Ande, R., Adebisi, B., Hammoudeh, M., Saleem, J. (2020)," Internet of Things: Evolution and technologies from a security perspective", *Sustainable Cities and Society* 54, 101728. <https://doi.org/10.1016/j.scs.2019.101728>.

- Andriotis, P., Oikonomou, G., & Mylonas, A. & Tryfonas, T. (2015), "A Study on Usability and Security Features of the Android Pattern Lock Screen", *Information and Computer Security*. 24. 10.1108/ICS-01-2015-0001.
- Appelt, D., Nguyen, C. D., Briand, L. C. & Alshahwan, N. (2014), "Automated testing for sql injection vulnerabilities: An input mutation approach", In *Proceedings of the 2014 International Symposium on Software Testing and Analysis, ISSTA 2014*, pages 259–269, New York, NY, USA ACM.
- Arbanas, K., & Hrustek, N. Ž. (2019), "Key Success Factors of Information Systems Security", *Journal of Information and Organisational Sciences*, 43(3), 131-144.
- Arun, R., Suresh, V., Madhavan, C. V., and Murthy, M. N. (2010), "On Finding the Natural Number of Topics with Latent Dirichlet Allocation: Some Observations," *Pacific-Asia Conference on Knowledge Discovery and Data Mining: Springer*, p. 391-402.
- Ayewah, N., Hovemeyer, D., Morgenthaler, J. D., Penix, J. & Pugh, W. (2008), "Experiences using static analysis to find bugs", *IEEE Software*, 25:22–29, Special issue on software development tools, September/October (25:5).
- Baskerville, R. (1999). *Investigating Information Systems with Action Research*. *Communications of the Association for Information Systems*, 2, pp-pp. <https://doi.org/10.17705/1CAIS.00219>
- Bertolino, A., Traon, Y. L., Lonetti, F., Marchetti, E. & Mouelhi, T. (2014), "Coverage based test cases selection for XACML policies" In *2014 IEEE Seventh International Conference on Software Testing, Verification and Validation, Workshops Proceedings*, March 31 - April 4, 2014, Cleveland, Ohio, USA, pages 12–21. IEEE Computer Society.
- Bishop, J.B., Bauer, K.W. & Becker, E.T. (1998), "A survey of counseling needs of male and female college students", *Journal of College Student Development*, 39, (2), 205-210.. *Journal of College Student Development*. 39. 205-210.
- Blei, D.M., Ng, A.Y., Jordan, M.I. (2003), "Latent Dirichlet Allocation", *Journal of Machine Learning Research* 3:Jan, 993–1022.
- Britten, N. (1995), "Qualitative Interviews in Medical Research", *BMJ (Clinical research ed.)*. 311. 251-3. 10.1136/bmj.311.6999.251.

- Cao, J., Xia, T., Li, J., Zhang, Y., Tang, S. (2009), "A Density-Based Method for Adaptive LDA Model Selection", *Neurocomputing* 72 (7–9), 1775–1781.
- Charitoudi, K., & Blyth, A. (2013), "A Socio-Technical Approach to Cyber Risk Management and Impact Assessment", *Journal of Information Security*, 4(1), 33-41.
- Chooi, S.T & Ahmad, K.M. 2017() " National cybersecurity strategies for digital economy. In 2017 International Conference on Research and Innovation in Information Systems (ICRIIS), pages 1–6. IEEE, 2017.
- Collet. S (2020), "What is security's role in digital transformation?" <https://www.csoonline.com/article/3512578/what-is-securitys-role-in-digital-transformation.html>, 2020. [Online; accessed 23-September-2022].
- Da Veiga, A., Martins, N. (2015), "Improving the information security culture through monitoring and implementation actions illustrated through a case study," *Computers & Security*, vol. 49, pp. 162–176.
- Deveaud, R., SanJuan, E., Bellot, P. (2014),"Accurate and Effective Latent Concept Modeling for Ad Hoc Information Retrieval. *Document numérique* 17 (1), 61–84. Dhillon, G. (Ed.), 1997. *Managing Information System Security*", Macmillan Education UK, London.
- DeWitt, A. & Kuljis, J. (2006), " Aligning usability and security: A usability study of polaris", *ACM International Conference Proceeding Series*. 149. 1-7. 10.1145/1143120.1143122.
- Dhillon, G., Oliveira, T., Susarapu, S., & Caldeira, M. (2016), "Deciding between information security and usability", *Developing value based objectives. Computers in Human Behavior*. 61. 656-666. 10.1016/j.chb.2016.03.068.
- Dhillon, G., Smith, K., & Dissanayake., I. (2021), "Information systems security research agenda: Exploring the gap between research and practice", *The Journal of Strategic Information Systems*. 30. 10.1016/j.jsis.2021.101693.
- Dhillon, G., Backhouse, J. (2001)," Current Directions in Is Security Research: Towards Socio-Organisational Perspectives", *Information Systems Journal* 11 (2), 127–153.
- Doukidis, G., Spinellis, S., & Ebert, C. (2020), "Digital transformation-a primer for practitioners", *IEEE Software*, 37(5):13–21, 2020.

- Duc, A. N., & Chirumamill, A. (2019), "Identifying security risks of digital transformation-an engineering perspective", In Conference on e-Business, e-Services and e-Society, pages 677–688. Springer.
- Eder-Neuhauser, P., Zseby, T., Fabini, J. (2018), "Malware propagation in smart grid monocultures Malware-Ausbreitung in Smart Grid-Monokulturen", *Elektrotechnik and Informationstechnik* 135 (3), 264–269.
- Flowerday, S. V., Tuyikeze, T. (2016), "Information security policy development and implementation: The what, how and who," *Comput. Secur.*, vol. 61, pp. 169–183.
- Glaspie, H. W., & Karwowski, W. (2018) "Human factors in Information Security Culture: A Literature Review", *Advances in Intelligent Systems and Computing*, 269-281.
- Gordon, L. A., Loeb, M. P., & Zhou, L. (2011), "The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?", *Journal of Computer Security*, 19(1), 33-56.
- Griffiths, T.L., Steyvers, M. (2004), "Finding Scientific Topics. Proceedings of the National Academy of Sciences 101 (suppl 1), 5228–5235.
- Han, D., Dai, Y., Tianlin Han, & Dai, X. (2015), "Explore Awareness of Information Security: Insights from Cognitive Neuromechanism," *Computational Intelligence and NeuroScience*, 1-11.
- Hassan, N. H., Ismail, Z., & Maarop, N. (2015), "Information Security Culture, A systematic Literature Review". The 5th International Conference on Computing and Informatics (pp. 456-463). Istanbul: the 5th International Conference on Computing and Informatics.
- Helsloot, I., & Groenendaal, J. (2011), "Naturalistic decision making in forensic science: Toward a better understanding of decision making by forensic team leaders", *Journal of forensic sciences*, 56(4), 890-897.
- Hess, T., Matt C., Benlian, A., Wiesböck, F. (2016), "Options for formulating a digital transformation strategy, *MIS Quarterly Executive*, 15(2).
- Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011), "Does Deterrence Work in Reducing Information Security Policy Abuse By Employees?", *Communications of the ACM*, 54(6), 54-90.
- Huang, A.H., Leavy, R., Zang, A.Y., Zheng, R. (2018), "Analyst Information Discovery and Interpretation Roles: A Topic Modeling Approach. *Management Science* 64 (6), 2833–2855.

ITU. (2017). Global Cybersecurity Index (GCI). Geneva, Switzerland: International Telecommunication Union.

Karjalainen, M., Sarker, S., Siponen, M. (2019.), "Toward a Theory of Information Systems Security Behaviors of Organisational Employees: A Dialectical Process Perspective. *Information Systems Research* 30 (2), 687–704.

Karjalainen, M., Sarker, S., Siponen, M. (2019)," Toward a Theory of Information Systems Security Behaviors of Organisational Employees: A Dialectical Process Perspective", *Information Systems Research* 30 (2), 687–704.

Karpunina, E.K., Konovalova, M.E., Shurchkova, Julia, V.S., Isaeva, Ekaterina, A., and Abalakin, A.A. (2019), " Economic security of businesses as the determinant of digital transformation strategy", In *Institute of Scientific Communications Conference*, pages 251–260. Springer.

Karumbaiah, S., Wright, R.T., Durcikova, A., Jensen, M. L. (2016), "Phishing training: A preliminary look at the effects of different types of training", In *Proceedings of the 11th Pre-ICIS Workshop on Information Security and Privacy*, pages 1–10.

Kraemer, S., Carayon, P and Clem, J. (2009), "Human and organisational constructs in computer and information security: Pathways to vulnerabilities," *Comput. Secur.*, vol. 28, no. 7, pp. 509–520.

Kumar, D., Sharma, A., Kumar, R., Sharma, N. (2019), "Restoration of the network for next generation (5G) optical communication network", In *2019 International Conference on Signal Processing and Communication (ICSC)*. IEEE; 2019. pp. 64–8. Search in Google Scholar.

Legner, C., Eymann, T., Hess, T., Matt, C., Bohmann, T., Drews, P., M"adche, A., Urbach, N., Ahlemann, F. (2017),"Digitalization: opportunity and challenge for the business and information systems engineering community",*Bus. Inform. Syst. Eng.* 59 (4), 301–308.
<https://doi.org/10.1007/s12599-017-0484-2>.

Li, P. L. , Amy, J. K., Andrew, B. (2020)," What distinguishes great software engineers? *Empirical Software Engineering*, 25(1):322–352.

Lubua, E. W., & Pretorius, P. D. (2019), "Ranking Cybercrimes based on their impact to organisations' welfare," *THREAT Conference Proceedings* (pp. 1-11). Johannesburg: THREAT Conference Proceedings.

- Lucila, N. B. (2016) , "Information Security Policy Development: A Literature Review," *Int. J. Innov. Res. Inf. Secur.*, vol. 3, no. 4, pp. 1–7.
- Lundgren, B., & Möller, N. (2017). *Defining Information Security*. *Science and Engineering Ethics*, 25(3), 1-8.
- Luo, A., Guchait, P., Lee, L. and Madera, J.M. (2019), "Transformational leadership and service recovery performance: the mediating effect of emotional labor and the influence of culture", *International Journal of Hospitality Management*, Vol. 77 No. 4, pp. 31-39
- Luse, A., Mennecke, B., Townsend, A., Demarie, S. (2013), "Strategic Information Systems Security: Definition and Theoretical Model," *AMCIS 2013*, August 15-17. Chicago, USA.
- Mahfuth, A., Yussof, S., Baker, A. A., & Ali, N. (2017), "A systematic literature review: Information security culture. nternational Conference on Research and Innovation in Information Systems", (ICRIIS), (pp. 1-6). Langkaw: International Conference on Research and Innovation in Information Systems (ICRIIS), Langkaw
- McFadzean, E., Ezingear, J.-N., and Birchall, D. (2006), "Anchoring Information Security Governance Research: Sociological Groundings and Future Directions," *Journal of Information System Security* 2(3), p. 3-48.
- Myers, M., and Newman, M. (2007), "The Qualitative Interview in IS Research: Examining the Craft," *Information and organisation* (171), pp. 2-26.
- Moeini, M., Rahrovani, Y. & Chan, Y.E. (2019), "A review of the practical relevance of IS strategy scholarly research",*The Journal of Strategic Information Systems*, 28(2).
- Morgeson, F. P., Aiman-Smith, L.D., & Campion, M.A. (1997), "Implementing work teams: recommendations from organisational behaviour and development theories, "In M.M Beyerlein, D.A. Johnson & S.T. Beyerlein (Eds). *Advances in interdisciplinary studies of work teams* (Vol 4, pp. 1-44). Amsterdam: Elsevier Science & Technology Books.
- Neuman, W. L. (2007), "Basics of social research": Qualitative and quantitative approaches(2nd ed.). Boston, MA: Allyn and Bacon.
- Paananen, H., Lapke, M., Siponen, M. (2020), "State of the Art in Information Security Policy Development", *Computers & Security* 88, 1–14.

- Padayachee, K. (2012), "Taxonomy of compliant information security behavior", *Computers & Security*, Vol 31, No. 2012, pp673-680.
- Samonas, S., Coss, D. (2014), "The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security", *Journal of Information System Security* 10 (3), 21–45.
- Sapronov, K. (2020). *The human factors and information security*. Kaspersky
- Sausalito, C. (2020), "Cybercrime To Cost The World \$10.5 Trillion Annually By 2025. New York", *Cybercrimme Magazine*.
- Sax, L. J., Gilmartin S. K. and Bryant A. N. (2003), "Assessing response rates and non response bias in web and paper surveys," *Research in Higher Education*, 44, 4, 409-431.
- Shahri, A. B., & Mohanna, S. (2016), "The Impact of the Security Competency on "Self-efficacy in Information Security" for Effective Health Information Security in Iran", *The Advances in Intelligent Systems and Computing*, 445, 51-65.
- Singh, S. & Hess, T. (2017)," How chief digital officers promote the digital transformation of their companies", *MIS Quarterly Executive*, 16(1).
- Siponen, M., Baskerville, R., Kuivalainen, T. (2005)," Integrating security into agile development methods", In: *Proc. of HICSS*.
- Sohrabi, N., Von Solms, R., Furnell, S., Elizabeth, P., and Africa, S. (2016), "Information security policy compliance model in organisations," *Comput. Secur.*, vol. 56, pp. 1–13.
- Soomro, Z. A., Shah, M. H., and Ahmed, J. (2016), "Information security management needs more holistic approach: A literature review," *Int. J. Inf. Manage.*, vol. 36, pp. 215–225.
- Stewart, H. (2020), "Information Technology and Cyber Security Unplugged": The interrelationship between Human Technology and Cyber Crime Today (English Edition), Rohhat LTD" 2020.
- Stewart, H. (2021), "The hindrance of cloud computing acceptance within the financial sectors in Germany", *Information and Computer Security*, Vol. ahead-of-print No. ahead-of-print. <https://doi.org/10.1108/ICS-01-2021-0002>.

- Stewart, H. (2022), "A systematic framework to explore the determinants of information security policy development and outcomes", *Information and Computer Security*, Vol. ahead-of-print No. ahead-of-print. <https://doi.org/10.1108/ICS-06-2021-0076>
- Stewart, H. (2022), "Security versus Compliance: An Empirical Study of the Impact of Industry Standards Compliance on Application Security", *International Journal of Software Engineering and Knowledge Engineering*, Vol. 32. <https://doi.org/10.1142/S021819402250015>.
- Stewart, H., and Jürjens, J. (2017), "Information security management and the human aspect in organisations", *Information & Computer Security*, vol. 25, no. 5, pp. 494–534. <https://doi.org/10.1108/ICS-07-2016-0054>.
- Stewart, H., and Jürjens, J. (2018), "Data security and consumer trust in FinTech innovation in Germany", *Information & Computer Security*, vol. 26, no. 1, pp. 109–128. <https://doi.org/10.1108/ICS-06-2017-0039>.
- Terglav, K., Ruzzier, M.K. and Kaše, R. (2016), "Internal branding process: exploring the role of mediators in top management's leadership–commitment relationship", *International Journal of Hospitality Management*, Vol. 54 No. 1, pp. 1-11.
- Thorwat, S. R. (2018), "ICT in Higher Education: Opportunities of Urban Colleges and Challenges of Tribal Colleges", *International Research Journal of Multidisciplinary Studies*, 1-6.
- Walsham, G. (2006), "Doing Interpretive Research," *European Journal of Information Systems* (15:3), pp. 320-330.
- WEF, W. (2019), "The global risks report 2019", World Economic Forum Switzerland, Geneva.
- Witmer, D. F. Colman, R. and Katzman, S. L.(1999), "From paper-and-pencil to screen-and-keyboard: Towards a methodology for survey research on the Internet, in Jones, S. (Ed.) *Doing Internet Research: Critical Issues and Methods for Examining the Net*. London. Sage. pp. 145-161.
- Zoto, E., Kowalski, S., Lopez-Rojas, E. A., & Kianpour, M. (2018), "Using a socio-technical systems approach to design and support systems thinking in cyber security education," 4th International Workshop on Socio-Technical Perspective in IS development (STPIS'18) (pp. 123-128). Tallinn]-Estonia: 4th International Workshop on Socio-Technical Perspective in IS development (STPIS'18).

Conclusion to STUDY 4: Digital Transformation Security Challenges

The fourth study addressed developing and implementing a secure digital strategy. According to the results of the study, a model for creating a secure digital strategy is based on eight elements that were examined and evaluated.

One of these elements was a top-down cybersecurity strategy that establishes several objectives and priorities to be completed within a predetermined time limit. The integration of secure software engineering tools, methods, and procedures into the software lifecycle is a component of secure systems engineering. The analysis and evaluation of security controls necessary to ensure the security of digital services and products are known as security testing and assessment—protection monitoring, which consists of both automatic and human security checks based on system or application-generated logs. An organisation's danger landscape can be seen in its entirety thanks to strategic advanced threat intelligence, which also contains strategic threat intelligence. In order to ensure optimal effectiveness, an incident response and remediation factor that comprises proactive, quick, and efficient issue response is also included.

The research also covered a thorough review of the factors affecting the overall strength or weakness of current security measures for digital strategies. In particular, managerial misperceptions about security, among other factors, contributed to a lack of security awareness among employees and detracted from the security culture (Parsons, McCormac, Butavicius, & Ferguson, 2010).

The results indicated that when managers understand the value of security in their digital transformation, their intention to invest in security is fostered, boosting employee morale. Apart from the importance of management involvement and employee acceptance of information security, the study also identified other factors such as threat vulnerability and risk assessment, which include threats, vulnerabilities and mitigation techniques that are linked to digital strategy and contribute to reducing overall risk.

Therefore, Study 4 dealt with the insufficient understanding of these key factors for digital transformation security that have led to a persistent risk to corporate information security and

addresses the study questions raised in Chapter 1 on the key factors that can strengthen cybersecurity in digital transformation and how they can lead to effective security outcomes.

The consideration of employees' involvement in the security chain and their perceived security in studies 1, 2 and 3 shows a strong influence of human behaviour on information security compliance. Considering the ambiguity of the intangible functions of different organisations, however, the question of how organisations manage their information security comes to the foreground: Do managers lack the skills to plan, train and direct human activities towards security awareness? On the other hand, if so, how do employees perceive the consequences of information security breaches and how do such breaches affect information security management? What kind of information security compliance policies should organisations adopt, and what key issues should these policies focus on? Furthermore, is there a correlation between technological and human factors that work together for the successful adoption and implementation of information security management in an organisation?

These are extremely important questions, but they have yet to be answered in the literature. It is also imperative to empirically investigate how and to what extent risk perception differs concerning humans and technology in different organisations, as the factors identified in this study play an important role in security and form a common attribute, namely a combination of humans (knowledge, education and training). However, the empirical research has yet to be validated. Study 5 explores this evidence and highlights the relationship between humans's perceptions of risk and the need to educate employees about the security of digital initiatives. Study 5 is discussed in the following chapter.

Chapter 8. STUDY 5: Information security management and the human aspect in organisations

Introduction

The fifth study is a continuation of studies 1, 2, 3 and 4. Using the data from studies 1, 2, 3 and 4, study 5 aims to provide a conceptual framework to facilitate the construction of a manageable information security system. While information services and technologies are critical to today's business environment, their interaction with humans poses a significant cyber threat. Consequently, unless management strategies are implemented to ensure that information systems are carefully deployed and managed, businesses will continue to face cyber threats that damage their reputation and place a significant financial burden on them.

Senior managers and employees are more likely to be sceptical of information provided to them, and their prudent behaviour to secure such information may be influenced by their perception of the criticality of the information given. It could be argued that their perception of cyber security affects how they use the information and how they disclose it to shape their expectations. The lack of strict information security policies and non-compliance leads to security failures in organisations (Ifinedo, 2014; Vance et al., 2012), usually triggered by poor management decision-making, employee engagement, collaboration and communication. Other factors, such as information security knowledge sharing and investment in information security, can influence employee behaviour towards compliance with information security policies and procedures.

However, previous research on IS security says little about how to close the gap between humans and IS. Study 5 fills these gaps by drawing on the findings of Studies 1, 2, 3 and 4 to propose a principle of information security compliance strategy that improves information security management by integrating human behaviours and IS security aspects in information security management.

Harrison Stewart authors the paper with contributions corresponding to the contribution ratio for this article, which is set out on the next page.

<https://doi.org/10.1108/ICS-07-2016-0054>

Statement of Authorship

CO-AUTHORSHIP APPROVALS FOR HDR THESIS EXAMINATION

PUBLICATION 5

This section is to be completed by the student and co-authors. If there are more than four co-authors (student plus 3 others), only the three co-authors with the most significant contributions are required to sign below.

Please note: A copy of this page will be provided to the Examiners.


Full Publication Details	Information security management and the human aspect in organization	
	Stewart, H. and Jürjens, J. (2017), "Information security management and the human aspect in organizations", Information and Computer Security, Vol. 25 No. 5, pp. 494-534. https://doi.org/10.1108/ICS-07-2016-0054	
Section of thesis where publication is referred to	Assistance with the comments of the journal editors (e.g. help with the clarity of the explanation of the results).	
Student's contribution to the publication	100 %	Research design
	100 %	Data collection and analysis
	99 %	Writing and editing

Outline your (the student's) contribution to the publication:

Harrison Stewart designed the research, conducted data collection and analysed the data. The text was written by him and I assisted him to revise some text to make it eligible for publication.

APPROVALS

By signing the section below, you confirm that the details above are an accurate record of the students contribution to the work.

Name of Co-Author 1 Jan Jürjens Signed  Date 12/12/22

STUDY 5

Information security management and the human aspect in organisations

Harrison Stewart, Jan Jürjens

Abstract

The rapid speed of Information Technology (IT) growth has created numerous business opportunities. At the same time, this growth has increased information security risk. IT security risk is an important issue in industrial sectors, and in organizations that are innovating due to globalization or changes in organizational culture. Previously, technology-associated risk assessments focused on various technology factors, but as of the early 21 st century, the most important issue identified in technology risk studies is the human factor. There are numerous proposals in the literature to remedy human and information security issues, but none have provided a comprehensive method to manage information security activities efficiently. To accomplish this, it is vital to have an in-depth understanding of the complex, dynamic, and unpredictable conduct of organization employees who direct and/or manage information security activities. In this paper, we present a conceptual framework and the Nine-Five-Circle principle (NFC) to enable organizations to implement a successful information security management strategy. The outcomes of this study can be used to improve the performance of information security management strategies in organizations

Keywords – Information security, Culture and technology, Employee behaviour in technology, IT, Human aspects, Security and leadership

Paper type - Research paper

1.0. Introduction

The rapid growth of Information Technology (IT) has increased security risks in both industrial and financial sectors. Currently, human activity is considered the most critical factor in the management of information security. Information security risks related to human activity is observed in employees from big and medium-sized businesses where employees violate company security policies or personally engage in security theft (Vance et al., 2013). These issues occur due to various factors such as poor information security awareness among employees, poor employee Information Security (IS) training, and poorly managed teams. These factors are major threats to a company's information security. Compliance to a company security policy and frequent IS training of employees can positively impact the human aspects of security. To eliminate the lack of security-awareness and deficiencies among employees so as to enhance their approaches to information security management, it is essential to take a deeper look into these factors.

In some organizations, the human resource department plays a major role in IT security by checking, controlling, and redirecting employee conduct toward successful information security management. Simply put, human resource departments are managed by an organization's management board, and the management board is responsible for planning, acquisition, IS training, and directing human activities in the business domain. This indicates that the management board is responsible for controlling and directing these activities to enhance the awareness of information security among employees. Although senior management alone cannot guarantee successful risk management, it is essential for senior management individuals to execute and control information security activities (Boss et al., 2009; McFadzean et al., 2006).

Organizational security policies are sets of rules and regulations that govern an organization's network, and they are intended to prevent fraud and embezzlement (Compston, 2009). These policies ban criminal activities – for example, an employee hacking into a computer system or network, employees visiting inappropriate websites, or the stealing of company software by/or enabled by employees. Puhakainen and Siponen (2010) argue that security-awareness training has a positive impact on employee conduct, and allows conduct to conform with the company security policy.

Compliance is defined as the conforming to a rule or a policy. We hypothesize that policies are not effective in an organization that lacks policy compliance (i.e. a policy is not effective in the absence of compliance). There are two components of compliance that should be highlighted: 1) Without

compliant employees, security policies are not guaranteed. 2) Compliance enhances the efficacy of information system security controls (Guo, 2013; Herath and Rao, 2009b). Harrison and White (2010) added that, compliance will only occur and be effective if enforced correctly by senior managers. However, according to previous studies, there are numerous managers who lack commitment to information security management, and this calls for education and persuasion via external or internal regulators (Ahmad et al., 2012; Chang and Ho, 2006; Hsu, 2009; Hu et al., 2007; Smith et al., 2010). Compliance analysis is the process of comparing the applied controls with the referenced standards. Furthermore, compliance analysis is a tool used for inspecting the conformity level of the business, and for finding problems that arise after the generated information security policies have been implemented. In any case, regardless of the possibility that the previously mentioned tools or techniques are used, they come short and do not cover the entire picture of information security management. Therefore, this study addresses the following questions:

1. Do the organizations' management boards lack the skills to plan, train and direct human activities toward security awareness?
2. What are the beliefs of employees regarding the outcomes of information security violations and how such violations affect information security management?
3. What kind of compliance guidance for information security do organizations need to adopt, and on what essential points should this guidance focus?
4. Is there any interrelation between technology and human factors that work together for the successful deployment and implementation of information security management in an organization?

We have answered the above hypothesis in their respective sections. In section 4 page 12, our findings and analysis will answer the research questions 1 and 2 and will be further illustrated in Table 4 (page 12 & 13). The third question will be answered in section 6 (page 16), where we will proposed our NFC principle that can be used to enhance the development and implementation of information security management policies in an organization. Section 6.2.3 (page 26) will answer our last hypothesis, whereby we confirm that technology and human factors are interrelated and work together for the successful deployment and implementation of information security management in an organization.

Information security policies have a major impact on the management of security and the success of a business. According to Trobec et al. (2007), the critical factor of information security is humans; however, there is always complexity in the interactions between humans and technical elements.

Trobec et al. (2007) argued that humans are the blueprint of information security, while Loster (2005) added that employee roles should be considered in the planning and implementation phases of information security policies and management. Therefore, in this study, we hypothesize that humans play a major role in security management, and this role should not be ignored.

1.1. The Gap

The massive advancement in the IT sector has increased the technological needs of organizations. With widespread use and access to World Wide Web services, security has become the most critical aspect for many organizations. Many researchers have proposed measures to solve these issues; however, the quantification of security measures is still considered a challenge by many studies. According to Yeniman et al. (2011), employee ignorance increases data breaches and data security vulnerabilities. In an empirical study conducted by Jaeger (2013) regarding the reasons behind data breaches, 38% of data breaches are due to loss of paper files; 27% are due to human carelessness (e.g., losing data memory devices); and the final 11% of data breaches are due to hacking. These data suggest that employees have a major influence on information security risk and data breaches. Rubenstein & Francis (2008) reported on the lack of compliance toward information security, as well as violations of access policies. Vance et al. (2013) argued that lack of IS training and policy violations occur due to unskilled or poor managers

1.2. Aim

The aim of this study is to encourage management boards to recognize that employees play a major role in the management of information security. Thus, these issues need to be addressed efficiently, especially in organizations in which data is a valuable asset. Engaging workplace employees in security awareness is a social event that also strengthens the security of a company's information. A strong company foundation in security awareness among employees ensures that employees are informed of company security policies. Employees trained in security awareness also improve innovation, and increase work productivity. Therefore, this current study also aims to highlight the importance of the formal and informal security awareness of employees to enhance employee productivity. In recent decades, many organizations have focused on technology-based solutions— e.g. intrusion detection mechanisms to address information security (PricewaterhouseCoopers, 2008). However, Safa et al. (2015) argued that, these approaches do not guarantee a secure business in the context of information security management. Furthermore, technology-based approaches often increase administrative and supportive costs and seldom dispose of the risk (Cavusoglu et al. 2009; Dhillon and Backhouse 2001; Siponen 2005). The implementation of such technologies can be tedious for employees when exploring information systems (IS) due to the informational gaps that come with software and hardware. Pahnla et al. (2007) also

argued that,

despite such huge investments, both software and hardware often do not decrease the security problems faced by these organizations. Numerous studies have also investigated how employees are targeted by hackers through different channels (e.g. social media); therefore, investing in multiple technology defense layouts have little impact on information security (Abawajy 2014; Arce, 2003; Jansson et al., 2013, Schultz et al., 2001 and Zhang et al., 2009).

1.3. Paper Structure

We began this paper with a brief introduction concerning the issues, the reasoning, and the need for this study, including the aims and objectives of the research.

In the second section, a literature review will be presented to analyze existing situations. This analysis will be based on the present study's findings, as well as analyses reported by other researchers. Gaps in current knowledge will be indicated, such as the lack of a single theory for poor security awareness.

In the third section, a conceptual framework will be developed to evaluate a security situation. Here, a questionnaire pertaining to the situation, with multiple choice answers will be prepared and provided to 600 individuals of varying ages, sex, field of employment, positions, designations, and income groups. The results of the survey will be quantified, and presented graphically. These data will help to identify major and minor causal factors between human aspects and information security risk.

The fourth section explores the methodology in which the proposed framework will be evaluated and verified via quantitative analysis. The reliability and validity of the findings will be further tested using statistical software tools (e.g. SPSS and SEM). These techniques will provide an outcome to fulfill the research aims. We hypothesize that lack of information security management training and lack of situational awareness among employees will be the top reasons for poor information security management.

In the fifth section, we present inferential limitations encountered during this study.

The sixth section will be based on the results from the methodology section. Herein, we will present a new compliance guideline based on the Nine-Five- Circle framework to enhance the deployment and implementation of information security policy compliance.

In the seventh section, we present the implications of this research, based on practice and future research possibilities.

The final section concludes with important points that organizations should consider when choosing IT security standards. We point out that the important points and suggestions generated herein may only work with specific types of organizations.

2.0. Literature Review

There have been numerous studies on information security management — for example, the information security viability model proposed by Kankan-halli et al. (2003), and the planning of security and risk management approach proposed by Soo Hoo (2000). Cavusoglu et al. (2004) and Mishra et al. (2004) studied investment in information security and assessment. While these studies have improved our comprehension of information security from different viewpoints, their outcomes have not been able to solve all the security issues that face organizations.

During the past decades, a significant amount of research has been done on numerous aspects of information security management – for example, external abuse (Simmonds et al., 2004 & Vivo et al., 1998), internal assaults (Guo et al., 2012; Harrington, 1996 & Straub et al., 1990), policies acceptance strategies (Siau, 2002 & Son, 2011) and computer crimes (Cronan, 2006). These studies indicate a great increase in the field of information security management research between the years 2000 – 2007 (Chen, 2010); however, much of this research focuses on internet abuse (Lim & Teo, 2005), individual behavior, compliance, and the impact of deterrence on employee conduct (Hovav & D'Arcy, 2012). Research on the organization level has not received a lot of attention. Lee & Kozar (2008) proposed the adoption of security technology and practices, while Siponen & Willison (2009) proposed traditional standard methods due to the complexity of security standards adoption. According to Kotulic & Clark (2004), the relative lack of firm-level research may mirror the reluctance of firms to uncover information with respect to their security strategies and breaches; subsequently, organizations choose to evade collaboration in security practices. Richardson (2011) demonstrated a drop in security personnel response to security measure surveys as compared to earlier studies. Numerous meta-analyses in data security have been done that recommend a holistic approach to dealing with current information security management issues. These studies propose several ways to deal with information security in order to have a bigger picture of information security. A few distinct frameworks have been proposed to address information security. These frameworks incorporate simulation models, formal models, dynamic models, and economic models for security (Dhillon & Backhouse, 2001; Siponen, 2005; Sunyaev et al., 2009).

2.1. Human role in Information Security

Other studies have also demonstrated that many organizations neglect the centrality of human behavior in information security management, and that this has caused failures in information security. Webb et al. (2014) proposed a situation aware ISRM (SA-ISRM) model to supplement the information security risk management (ISRM) procedure, however, their model was only focused on the deficiencies of ISRM. Here, the researchers neglected security policy compliance based on individual employees. Li et al. (2010) argued how recent studies on information security management have neglected the perceived benefit of degenerate behavior, individual norms, and organizational settings. Their research model utilized an online survey that was sent to organization employees. However, their work was only based on internet use policy (IUP) compliance. Thus, they focused on employees in an organization with an internet use policy and realized the risks posed by employees in the context of security management in an organization. They also recommended the significance of considering compliance decisions as driven by a cost-benefit analysis, limited by individual standards and organizational setting factors. Therefore, their work did not cover all the elements of human behavior and social structure in the organization, such as human ability, culture, IS management, top personnel, technology, and how all these factors interrelate and work together. Here, we emphasize that both Li et al. (2010) and Webb et al. (2014) indicate the limitations of a number of theory- based empirical studies on employee security policy compliance that we address in this study.

Da Veiga and Martins (2015) conducted a questionnaire survey where they studied the interrelationship between human, technology, and strategy controls. Their data was derived from information security culture assessment (ISCA), based on a case study of an international financial institution at four intervals over a period of eight years, across twelve countries. Their study was centered on the effects of security-awareness training, and they recommended further research to be conducted on employees who comply to information security policy and others who do not, as well as extending the research across national and cultural boundaries.

Herath and Rao (2009) argued the need for organizations to deploy different approaches to enhance data security. Ifinedo (2012) added that many organizations are heavily investing in technology- based measures, but these often do not yield positive results due to the lack of attention allotted to employee behavior. Crossler et al. (2013) concluded that a combination of technology-based solutions and

employee security behavior plays a major role in information security management, and this calls for a strategic approach to model a solution to unify technology, human, cultural and organizational factors.

2.2. Technology role in information security

Numerous studies have investigated cyber-attack prevention. According to Li et al. (2009), limited countermeasures are available to prevent cyber-attacks. Mirkovic and Reiher (2005) proposed the source-end defense points. Chen and Hwang (2006) also proposed the core-end defense techniques, while Wang et al. (2007) proposed the casualty end protection, and Seo et al. (2013) proposed the versatile probabilistic filter planning. All the above countermeasures have been developed to prevent flood attacks, but none were aimed at employees. Other traditional techniques such as; cryptography and firewalls have also been proposed as distinct options to avoid intruders and maintain data confidentiality, integrity, and authentication (CIA) (Wright et al., 2004). According to Singh et al. (2013), technology is not capable of providing a dependable answer for hierarchical information security needs and challenges. Werlinger et al. (2009) recommended that, to overcome the constantly challenging issues of information security management, it is important that in combination with a technical approach, employee and organizational factors should also be addressed. In their recommendation, the technical approaches are initiating, planning, acquisition of new innovations, budgetary designations, and purchasing innovative hardware and software. Human factors include skilled staff recruitment, hiring, information security management training and employee motivation. Organizational factors include staff compliance with organization rules and regulations, frequent information security management training, rigid managerial direction, and the presence of compliance departments. Hence, we hypothesis in this study that technology and human factors are interrelated and need to be addressed efficiently for the successful deployment of information security management (Werlinger et al., 2009; Abawajy, 2014; Arachchilage and Love, 2014; Kritzingner and von Solms, 2010).

2.3. The financial impact on information security

According to Safa and Ismail (2013), information security breaches cause financial costs for organizations as well as impact organization reputation. In addition to adopting technology-based solutions, appropriate data security conduct can mitigate the risk of information security breaches in an organization. Abawajy (2014) determined the important role of security compliance awareness among employees, such as conduct and behavior during a study on security risk mitigation. This research was subsequently supported by findings generated by Arachchilage and Love (2014). However, both researchers neglected human ability, culture, information security management, technology and how

all these variables interrelate and need to be addressed efficiently in an organization. Kritzinger and von Solms (2010) held a workshop where they divided users into home and organizational environments to confirm the important role that both groups play in security awareness. They further confirmed the efficacy of the methods utilized and the strong impact of policy enforcement. However, Kritzinger and von Solms (2010) based their study on private and public behavior, but neglected culture, familiarity, management, technology and how all these factors interrelate and work together. Safa et al. (2015) found that knowledge of information security (IS) is linked to better understanding, familiarity, and the capacity to manage and overcome crises.

2.4. Misuse of information security knowledge sharing

The misuse of IS resources has been recognized in numerous studies as a significant problem, often identified during information security mitigations. This supports the hypothesis found in other studies that assessed employee behavior, that workers often take part in inappropriate behaviors increase security risks. These findings caused many organizations to concentrate on placing impediments and preventative systems such as sanctions on employees for the misuse of computers. Straub and Nance (1990) explored how to detect computer abuse, and how to sanction employees. They advised organizations to sanction employees severely to prevent other employees from conducting the same or similar activities. Willison (2006) studied the impacts of employee misbehavior and subsequent risks for information security by utilizing rational decision and crime preventive methodologies to explore the relationship between the culprit and the context. According to Willison, organizations need to concentrate on the inappropriate behavior of employees in various levels and enforce preventive measures to decrease employee behaviors that increase information security risks.

A study by Lee and Lee (2002) focused on the deterrence hypothesis along with social speculations to clarify the impact of information security management, information security programs, and organizational factors. Lee and Lee (2002) analyzed both insider and outsider information security abuse by evaluating organizational factors and the causes of the security abuse. They determined that the improvement of social networks via organizational factors could eliminate the misuse of information systems in an organization. However, Lee and Lee based their work on how social relationships and traditional counter-measures impact the decision process employees that misuse computers by utilizing the General Deterrence Theory (GDT) for guidelines (e.g., as in the work of Straub and Nance (1990)). The GDT is a basis for security awareness, security training and education

and minimizes cost (Beccaria, 1963), however, it comes with some limitations and needs to be enhanced and revised. GDT also neglects the interrelationship between technology and humans.

2.5. Information security management standards

Siponen and Willison (2009) analyzed BS7799, PCI BS, ISO/IEC17799: 2000, GASPP/GAISP, and the SSE-CMM to determine and compare how international information security management guidelines play a key role in managing and confirming the organizational information security. They realized that those listed guidelines were too generalized and neglected the verification of the difference in information security requirements in various organizations. Furthermore, these guidelines were not meant for international IS standards because of their general practices in nature. Due to these shortcomings, they recommended that information security management guidelines should be seen as “a library of material for information security management for specialists” (Siponen and Willison, 2009). An empirical study was conducted by Kotulic and Clark (2004) in the sector of security risk management (SRM) where they proposed a conceptual model to enhance SRM on organizational level. However, their model was not able to detect and specify information systems security. According to Baskerville (1993), computer misuse (i.e. use for purposes other than that intended by the company, such as recreational activities) is the main cause of information security risk, and they recommended that information security experts and IT managers should implement systems that will detect information security abuse and specify information systems security.

Despite the fact that the vast majority of the data security literature focuses on sanctions and technology-based solutions, there is little data on the roles management boards, employee IS training and collaboration play in information security management. The current study will not only evaluate technology and the responses of individual employees, but will also target individual managers because they are responsible for the proper implementation of security compliance. Our study further analyzes organizational culture, collaboration, employee familiarity with security management, managing director skills, governance, leadership, records management, information access, communication, compliance, technology, and how all these factors interrelate and work together. The expectation is that security compliance needs to be initiated from the top level down to the lowest level in every organization.

In our work, the factors in our research are both dependent and independent factors. These factors are interrelated and complex design reflects that a number of independent factors may work together to

determine the level of dependent factor. For example, we investigate the cause of the issues that an organization faces during policy compliance deployment (the dependent variable). Here we hypothesize that our SPSS findings such as, lack of security training-awareness, lack of management directives, absence of compliance policy, lack of security interest and hardware failure (five independent factors) may work separately or in conjunction with each other in determining the condition of the dependent factors. The identification of independent and dependent factor relies on the particular research question and conceptual underpinning of our work. Here, the two labels "dependent" and "independent" can be used in a specific design differently from ours. That is to say, there is nothing inherent in a factor itself that makes it independent or dependent; a factor that is an independent in our design may in another work be used as the dependent factor or the effect of estimation.

3.0. Method

Uneducated employees and/or unethical employee behavior are causes of information security risk (Abawajy, 2014; Arce, 2003). It is clear that security risk cannot just be eliminated solely via security-awareness without effective implementation and enforcement of compliances by organization management boards. In this study, we first analyzed levels of employee information security awareness regarding information security risk via their observational and behavioral viewpoints. We were also aware that employee awareness of information security does not guarantee that they will be compliant; therefore, we extended the scope of the study to analyze top management board individuals' information security awareness, and proposed an effective information security policy compliance guideline.

We developed a conceptual framework, illustrated in Figure 1, using the SBT, to explain how employees comply with information security policies.

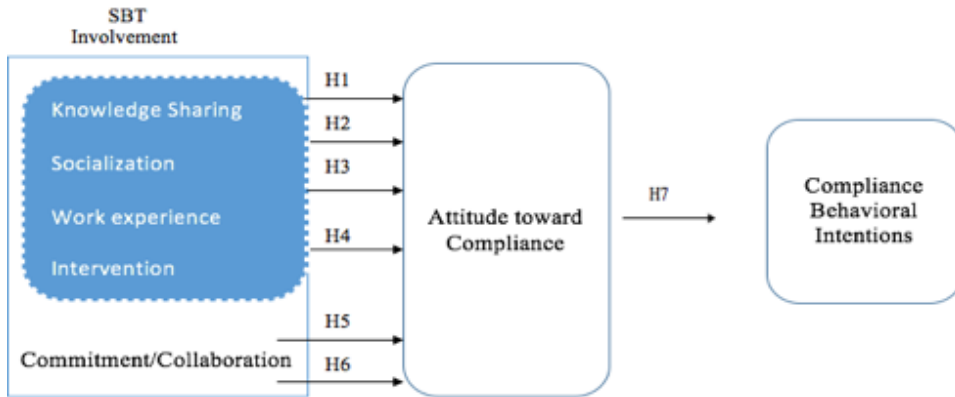


Figure 1. A conceptual framework

Before developing the instrument for the survey, we first identified and developed effective measurements built upon the existing literature, prepared our survey questionnaires according to past studies, and analyzed our findings based on previous qualitative analyses. We were able to collect data by utilizing a cross- sectional questionnaire and a Likert scale as in the work of Ifinedo (2014) and Witherspoon et al. (2013). All surveyed questions shown in appendix.1 are related to an item illustrated in Table 1. Data analysis was conducted with SPSS as described in the SPSS Analysis diagram in Figure 2.

Table 1. Questionnaire and related items.

Question Related Items	Description
Knowledge and Information Management (KIM)	Q1 - Q30 are related to how the employees value and use information in the company. For example, if they are aware of KIM and who is responsible for their organization KIM as well as how their organizations have assessed and identified critical information.
Records Management	Q31 - Q38 are related to how organizations keep records, share information, destroy and dispose created information. Furthermore, they are also related to the responsibility of record management and their storage, the sustainability of digital records, retention procedures, disposal policies and how data is transferred.
Information Access	Q39 – Q44 are related to how these organizations secure data and re-use data, how they meet freedom of information (FOI) requests

	and if they are aware of their technical environment that enhances their information.
Compliance / Governance and Leadership	Q45 – Q62 are related to change management programs that are held in the organization. Subsequently, change management programs and clarified procedures that enable them to examine completeness, availability and usability of data asset after any change. The questions are also related to IS training, induction programs, staff responsibilities, change management, policies and guidance. We also wanted to be informed on governance and leadership in these organizations such as: any naming conventions that are mandatory to abide by as well as their strategic management, business objectives, resourcing, risk management and management supports and control.
Culture	Q63 – Q69 are based on both individual and organizational culture. Furthermore, these questions are also related to employees commitment, knowledge sharing, collaboration, communication and understanding. For example, how effective is the sharing of knowledge enhances KIM networks, communities and if there are several strategies that have been adopted to enhance internal communication and collaboration in these organizations.

3.1. Data collection

In Germany, we approached different organizations that ranged in both size and how they approach information security management. We then divided the three participating organizations into cases: CASE 1, a PRIVATE BANK with over 1500 employees; CASE 2, an AUTOMOBILE manufacturer; and CASE 3, a FINTECH startup company with 125 employees. Participants were requested to answer different questions, including demographic information including age, gender, and position. We focused on data from the senior directors, functional managers, IT specialists, and personnel in all three organizations. All participants had internet access and utilize the internet in various departments..

A preliminary workshop for a pilot test explained the questions to the participants and ensured that each participant understood the purpose of the research study. Each question was explained in various

ways to ensure that all questions were understood in the same manner by all participants. After this phase, participants were asked to answer the cross-sectional questionnaire survey composed of closed-ended questions. These questions were intended to gather and measure quantitative data on a diversity of interests.

We applied the Microsoft © Access Management Matrix that helped us to determine what data would be needed for this study, and from whom to collect these data, by listing all management levels vertically and department levels horizontally. Due to data policy, an agreement was written and signed by the researchers stating that the collected data would only be used for this study and would not be shared with any third party. After they agreed to the terms and conditions, we presented them with the questionnaires. The pilot testing during the initial phase assured that all participants understood the questions. The pilot test consisted of 70 questions, compared to the 50 questions in the final version shown in Appendix 1. Time spent on social media sites via utilizing company computers and networks was questioned as well. The role of employees in information security breaches as well as their adherence to security policies were also asked. A comment field was added in the form for participants to share their experiences, worries, and the reasons that drive them not to abide by information security policies.

We extended the standard data collection and sped up collection by sending a link of the website form via a mass mail to all other participants. The top personnel were asked how they view their roles in information security management and infrastructure development. They were also asked how they manage their security policy, how they see the role of human factors in information technology, and how they train their personnel on information security risks. The surveys took an estimated 45 minutes to complete. All answers were saved in a MySQL database.

3.2. Demographics

The reason for this research was to explore Information Security (IS) management, explore the human aspect in organizations and to propose a compliance guideline for organizations. We mailed a total of 955 questionnaires to participants using mass mail software, and received 633 completed responses. These data were saved in a database for further analyses. We also printed 100 copies and distributed them to other participants, so that our answered questionnaires totaled 733, which enabled us to analyze the data.

Table 2. Demographic of participants.

Variables		TOTAL
Gender		
	Male	60%
	Female	40%
Age		
	18-30 years	20%
	31-40 years	35%
	41-50 years	40%
	50 + years	5%
Position		
	Senior Directors	15%
	Functional Directors	20%
	IT Specialists	15%
	Personnel	50%
Participants from each CASE		
	CASE 1 - Bank	60%
	CASE 2 - Automobile	25%
	CASE 3 - FINTECH Startup	10%

Table 3. Demographics of respondents based on educational level.

Level of Education		Group			TOTAL
		Academic	Administrative	Students	
Elementary School	Number	0	15	0	
	Percentage	0.0	1.14	0.0	
Secondary School	Number	0	33	0	
	Percentage	0.0	2.5	0.0	
High School	Number	2	211	0	
	Percentage	0.15	16.05	0.0	
Associate Programs	Number	3	27	776	
	Percentage	0.23	2.05	59.1	
HND	Number	2	19	0	
	Percentage	0.15	1.4	0.0	
Bachelor	Number	59	21	0	
	Percentage	4.5	1.6	0.0	
Masters	Number	37	5	0	
	Percentage	2.81	0.4	0.0	
PhD	Number	95	9	0	
	Percentage	7.2	0.27	0.0	
TOTAL	Number	198	340	776	1314
	Percentage	15.06	25.87	59.1	

3.3. Results

We utilized a structural equation model (SEM) as was conducted in Hair et al. (2010) because of the simplicity and accuracy of this type of model. SEM has various methodologies that enabled the depiction of relationships among variables. It also provided a quantitative sample of our proposed model (Table 2). Furthermore, because our work in this study was based on past literature reviews, involvement theories, and social hypotheses, we utilized the three fundamental methodologies of SEM: confirmatory factor analysis; regression analysis; and path analysis, similar to the work of Schumacker & Lomax (2010). Certain variables that could not be observed, such as collaboration, job contentment, employee devotion, work experience, socialization, creativity, knowledge sharing via SNS, commitment and others, were measured by few items. These variables were considered as latent variables which were then modelled utilizing both the structural and measurement models within SEM. Following the work of Gaur (2009), our measurement model focused on the relationship that exists between the variables we observed and those we classified as latent, while our structural model focused on the latent variables.

4.0. Findings and Analysis

In all three organizations in our study, we found that the main issues that trigger security incidents, and that hinder the accomplishment and enhancement of information security compliance were based on different factors. For example, we found that employee behavior is the most common obstacle associated with information security compliance (e.g. password sharing, password written down on a piece of paper, utilizing shortcuts, visiting unauthorized websites, downloading unapproved internet programs from the internet, opening unapproved email attachments, disregarding important security strategies, lack of knowledge, poor IS training, keeping relevant information to themselves, lack of commitment, lack of security awareness, security infringement(s) not reported, culprit(s) not punished, weak security-related guidelines, and lack of security compliance regulations). On the organizational level, we found that employees do not comply with organization rules and regulations due to lack of organization handbooks with clear rules and regulations, as well as lack of IS training, lack of managerial direction, and the absence of compliance departments. On the technical level, we found that both the Automobile and the Bank institute were still utilizing legacy technology devices and traditional information security management standards that do not meet their needs.

Furthermore, we realized that in all the organizations, employees were reluctant to share knowledge or collaborate in the context of information security. The FinTech organization lacked effective IS training courses, absence of workshops, lack of security notices, lack of monthly mass-mails in the context of information security, lack of company social network web page, and lack of general company procedures. All these findings answer research questions 1 and 2 as illustrated in Table 4..

Table 4. Causes of Security Incidents and Hindrance

Organizations	Causes	Hindrance
Bank		
	Poor or ill management, employee errors, and noncompliance.	Due to poor security “know-how” and “know-why”. Lack of security awareness and training respectively. Poor administrative directives and/or roles.
	Access violation: malicious and/or viral software.	Poor organizational structure. Lack of knowledge on whom to contact and the absence of clear definitions of security process and roles. Lack of collaboration, communication, and commitment.
	Not complying with organization rules and regulations.	Lack of security compliance regulations and lack of security policy compliance training.
Automobile		
	Poor or ill management, employee errors, and noncompliance,	Due to poor security “know-how” and “know-why”. Lack of security awareness and training respectively. Poor administrative directives and roles. Lack of collaboration, communication and commitment.
	Access violation: malicious and/or viral software.	Poor organizational structure. Lack of knowledge on whom to contact and the absence of clear definitions of security process and roles.
	Not complying with organization rules and regulations.	Lack of security compliance regulations and lack of security policy compliance training.
	Sharing passwords and engaging in private social networks and/or emails.	Lack of security awareness; security infringement(s) not reported and culprit(s) not punished.
FinTech Startup		
	Poor or ill management, employee errors, and noncompliance.	Due to poor security “know-how” and “know-why”. Lack of security awareness and training respectively. Poor administrative directives and roles.
	Access violation: malicious and/or viral software	Poor organizational structure. Lack of knowledge on whom to contact and the absence of clear definitions of security process and roles. Lack of commitment.
	Hardware failure(s).	Budget constraint(s).

To determine if my conceptual framework and findings describe employee information security activities that occur over the span of managing day-to-day activities, I utilized the SPSS statistical software to develop an in-depth visual evaluation of the findings. This visual evaluation enabled me to detect patterns and relationships that exist with employee information security-related conduct in the three organizations. The SPSS analysis produced the results that satisfied my main research aim.

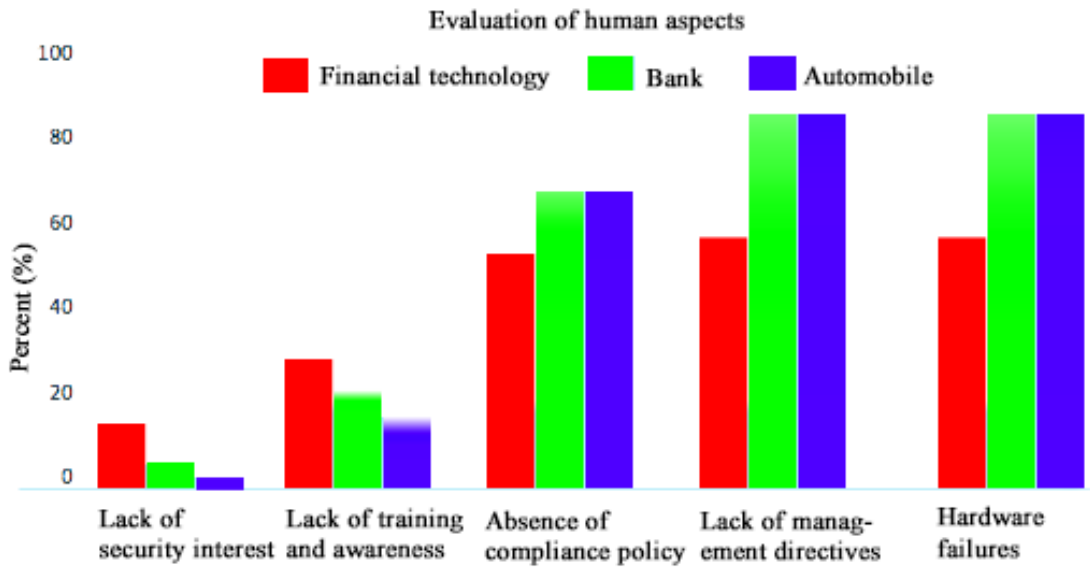


Figure 2 – SSPS Analyzer

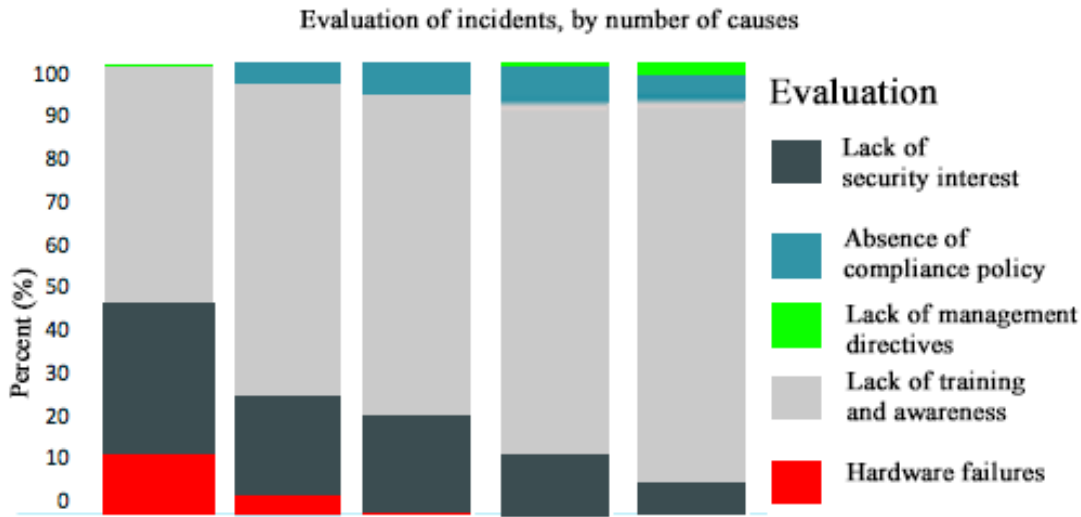


Fig. 3 Stacked chart

As shown in Figures 2 and 3, the primary driver of security risk is not just employee error, but also lack of IS training and unskilled management boards. The head of the IT manager at the Bank stated that human errors are the main issues of the bank, e.g. employees downloading unauthorized software that many contain viral and/or malicious data and/or programs. The Data Protection Unit manager also stated that lack of IS training has become a problem that need to be addressed. He added that the heads of the organization consider security training as a waste of investment. The head of the management board added that most security training costs large sums of money, yet have not delivered results or improvements.

We also identified that both the Automobile company and the FinTech startup had difficulties with administrative errors and security managers. Most of their security managers are bachelor degree holding individuals that have no or low experience in real world information security management. The FinTech company also had budget constraints that hindered them from implementing strategic security mechanisms and/or a process to enhance or protect organizational data. Other attributes such as budget constraints, operation, organizing, budgeting, time- frame, managing and reporting procedures, and the cost of security training and outcomes were all part of our findings.

Our literature review and results indicate various aspects of administering information security management in different contexts. We focused on human aspects in information security management, technical factors, organization policies, employee security-awareness training, technologies adopted, employees' collaboration and commitment to the organization, the activities of the management boards, and how security is viewed in their business domain. From this we cannot simply conclude that information security awareness will keep data safe without training the employees on this subject. Training the employees on information security management can enable employees to know why security is important; however, lack of compliance in this context will not make this training effective at reducing security breaches. Various studies have focused on both security awareness and security training, but none has been able to solve the security issues that these organizations currently face.

We present a comprehensive information security management plan based on the Nine-Five- Circle that ensures the transfer of knowledge regarding information security and potential threats to organization data assets. According to Hagen et al. (2008), increasing knowledge in security awareness is more effective at increasing policy compliance than other information security management measures. Albrechtsen & Hovden (2010) added that IS training directs and enhances employee behavior towards policy compliance. Siponen et al. (2014) argued that without employees complying

with security policies, security-awareness training will not be an adequate solution. It is therefore clear, that employees need to be trained on policy compliance. Ma et al. (2009) highlighted this, and further studied the essential role that compliance training has on information security management.

Rubenstein & Francis (2008) studied how policy compliance can prevent access policy violations. Parson et al. (2014) studied how compliance training has had various positive effects on numerous organizations.

5.0. Study limitations

We encountered limitations during this study. Some of the data collected were from organizations that were externally regulated. The FinTech external regulator initially disapproved the project due to risk management (i.e., not realizing finance and risk alignment benefits). The external regulators believed that the FinTech organization lacked the capability needed to execute compliance policies successfully in the real world. It was a tedious task to acquire authorization from these regulators for surveys and data collection in the area of information security. In any case, the data we collected were enhanced with a greater sample size by including the other organizations.

Due to information security management unawareness of employees, some of the staff members at the bank resisted the survey (Joshi, 2005). These staff members did not comprehend the importance of our research due to changing and new challenges in IT security risk that have arisen in recent years (Pan and Kim 2006). This could have been solved via another workshop to explain the reason behind this survey.

Another critical problem in our study came from the failure to control for duplicated responses by employees that took part in the online survey. Such issues could be mitigated in the future by ensuring that each person enters his or her email address as well as recording the employee MAC or IP addresses. With this approach, we could have identified employees with multiple responses or prevent duplication from occurring.

6.0. Compliance guidelines and decision making

Globalization and emerging markets have increased the complexity of information sharing. This complexity has also increased security risks, which has become a large issue in many organizations' information security management. Recent studies have depicted how organizations are deploying technology solutions and other strategies to eliminate these risks. From our findings, none of these

approaches yielded positive results, while some organizations are not even aware of the importance of data security. On the other hand, modern organizations rely on information to make decisions that are used to carry out organizational activities. In this section, we answer our third research question by proposing a principle that will enhance the development and implementation of information security management policies in an organization. This will also help eliminate various issues with respect to information security management and help to enhance productivity in an organization. There are numerous ISRM standards but not limited to the ISO27000 series (ISO27001, ISO27002), SAS70, SOC2 and PCI DSS. In this work we propose a new principle called the Nine-Five-Circle (NFC) that can be configured to meet individual organizational needs. The proposed principle will indicate the necessities for the implementation of operational and information security enhancements. It also puts more emphasis on the measurement and evaluation of organization ISMI performance and outsourcing. We can relate our principle to the ISO27001:2013 and supersedes the ISO27001:2005 (Bresin & Paul, 2014; Mackie & Ryan, 2013; Herbet & Chantal, 2014). The NFC prescribes an administration model to empower organizations in planning and vigilance in:

- How information systems are understood and how those systems identify critical events.
- What security counter measures have been deployed for information protection.
- How valuable data assets have been identified and how they are protected.
- What process the organization has utilized to identify applicable legal, regulatory, and other obligations.

Specific guidelines are not provided by NFC; however, it enables organizations to manage information security in an organized way by providing a principle to enhance the management of security measures, potential risks, uncertainty, unpredictable incidents and compliance.

At this phase of our study, we cannot conclude that the standard ISO27001 and ISO 27002 will fit organizations that are eager to identify or detect potential risk. This is due to the fact that, utilizing the ISO 27001 standard checklist would be excessively specific and would decrease flexibility in processing information security management tasks in this study. The ISO 27001 is presumably the most well known of all the ISO standards due to the essential tools it provides to enhance security of information. For example, one of the greatest myths about ISO 27001 is that it is centered around IT; however, we cannot agree to this because IT cannot secure information alone. In the context of security, human resource management, physical security, legal protection, organizational issues and how they are interrelated are required to secure information as in the context of the NFC principle.

Therefore, this study proposes the NFC to support the general procedure of information security management by taking not only IT into consideration but also human resource management, physical security, legal protection, organizational issues and how they are all interrelated to secure information. We propose that an organization following the NFC principle can effectively measure their risk and deploy robust security measures based on their needs. As in the case of the ISO 27001, an organization can select from the 114 controls, which will provide instruction on what an organization needs to accomplish, yet does not provide the information on how this should be accomplished. Moreover, these 114 controls can be misleading since the implementation guidance prescribes various actual controls in the details. This is the purpose of the ISO 27002, which provides more details on implementation. However, an organization cannot use only the ISO 27002 because it does not provide any information about which controls should be implemented, how to measure them, or how to assign them to the right humans. The ISO 27002 is an advisory document and not a formal specification like the ISO 27001.

6.1. Our proposed Principle (NFC)

The NFC principle is defined as a strategic diagram that shows the potential factors that prevent the successful development and implementation of an information security management strategy. This principle is mainly a process used to design, to identify, and to mitigate potential factors causing an overall hindrance in security-related policy compliance within an organization. Every potential factor that generates any hindrance is a cause of variation that should be addressed.

In Table 4, we defined several incidents that hinder information security management in organizations through our data collection and findings. In this section, we propose a principle that enhances the interrelationship between technology and human factors in an organization for the deployment of successful information security management (Werlinger et al., 2009; Abawajy, 2014; Arachchilage and Love, 2014; Kritzinger and von Solms, 2010). In this work, we derived five causes and hindrances after analyzing the data using SPSS, as depicted in Figure 2 and Figure 3. These causes and hindrances are: 1) lack of security interest; 2) lack of security-awareness training; 3) lack of management directives; 4) absence of compliance policy; and 5) hardware failures. We then propose the NFC principle to solve those issues, rather than using any general standard guidelines that has been proposed in the literature thus far. The NFC principle should enable us to come up with a moderate procedure for successful development and implementation of an information security management strategy based on organizational needs. In this work, the comprehensive nature of the NFC principle should enable us to

enhance the interrelationship of technology and human factors highlighted above, and to close the knowledge gaps that still exist for the deployment of a successful information security management strategy. Figure 4 introduces our NFC principle with the five causes and hindrances we derived from the SPSS analysis. These causes and hindrances are grouped into attributes and categorized as potential key factors. The key factors are held together by the central point of the NFC that consists of all the prerequisites that are essentially needed for the development and implementation of the ISRM. In our work, we developed a conceptual framework, illustrated in Figure 1, using the SBT to explain how employees comply with information security policies. Here, the variables that were not observed, such as job contentment, employee devotion, work experience, socialization, creativity, knowledge sharing via SNS and commitment are considered as our latent variables as shown in Figure 6. Other prerequisites include, but are not limited to, collaboration, cultural, confidentiality, integrity, moral agreements, certified leaders, and communication. Therefore, our prerequisites (including our latent variables) are the blueprint in the development and implementation of ISRM in the concept of the NFC. These prerequisites are the shaft on which the NFC oscillates. The key factors are joined together by a dynamic compliance process standard that involves: A) awareness of the compliance regulation; B) controlling integration; and C) closing gaps. Both the key factors and the central point prerequisites are enclosed in the control integration and close gaps dynamic. The rotation starts at the 9 o'clock, 12 o'clock, 3 o'clock, 5 o'clock, and 7 o'clock positions. The entire process repeats itself after each lifecycle during a time span and needs to be adjusted frequently. .

6.1.1. Why The NFC

The NFC is a portable, simple and improved starting point when compared to other principles and frameworks, such as the standard ISO27001 and ISO27002, which come with different distinct features. For example, the ISO 27002 does not make a distinction between controls applicable to a particular organization and those which are not, while the ISO27001 prescribes a risk assessment to be performed in order to identify for each control whether it is required to decrease the risks, and if it is, to what extent it should be applied. Here, we can see that both standards are different, but lack the positive attributes of both tools when combined. This is where the NFC comes in, taking usability in to consideration and utilizing a single standard that makes it simple and portable for practical use. The NFC also focuses on design, identification, and the mitigation of potential factors causing an overall hindrance to security-related policy compliance within an organization. Every potential factor that generates any hindrance is a cause of variation that should be addressed in the NFC context, unlike the

ISO27000 where standards are designed for certain focus. For example, the ISO27001 is for building an IS foundation in an organization, the ISO 27002 is for the control implementation, and the ISO 27005 is for carrying out risk assessment and risk treatment. The NFC combines all these with a dynamic compliance process standard that involves: A) awareness of the compliance regulation; B) controlling integration; and C) closing gaps. Both the key factors and the central point prerequisites are enclosed in the control integration and close gaps dynamic. The NFC also enhances the interrelationship between technology and human factors and these are not seen in the context of ISO27000. In this paper, Figure 4 introduces our NFC principle with the five causes and hindrances we derived from the SPSS analysis.

6.2. Applying the NFC in this study

As shown in Figure 4, the five key factors (lack of security interest, lack of IS training and awareness, lack of management directives, absence of compliance policy, and hardware failures) are all joined with the central point. Security training and awareness have been separated on our SPSS results in Figures 2 and 3 because employees might be aware of security issues but without training, they might make costly errors in regard to information security. Therefore, security-awareness training should be implemented to reduce or eliminate costly errors among employees in the context of information security. Here, the security- awareness training includes, but is not limited to, workshop training sessions, security programs, security awareness websites, or emailed information. All these procedures are capable of enhancing employee understanding of organizational security policy, process, and best practices.

Starting from the 9 o'clock position, we have placed our first key, lack of security interest, followed by lack of security-awareness training and awareness, lack of management directives, absence of compliance policy, and hardware failures. In the NFC, it is essential to address the SPSS analysis results efficiently based on how critical each key factor is assessed, and how they affect other key factors by taking the needs of the organization into account within each lifecycle.

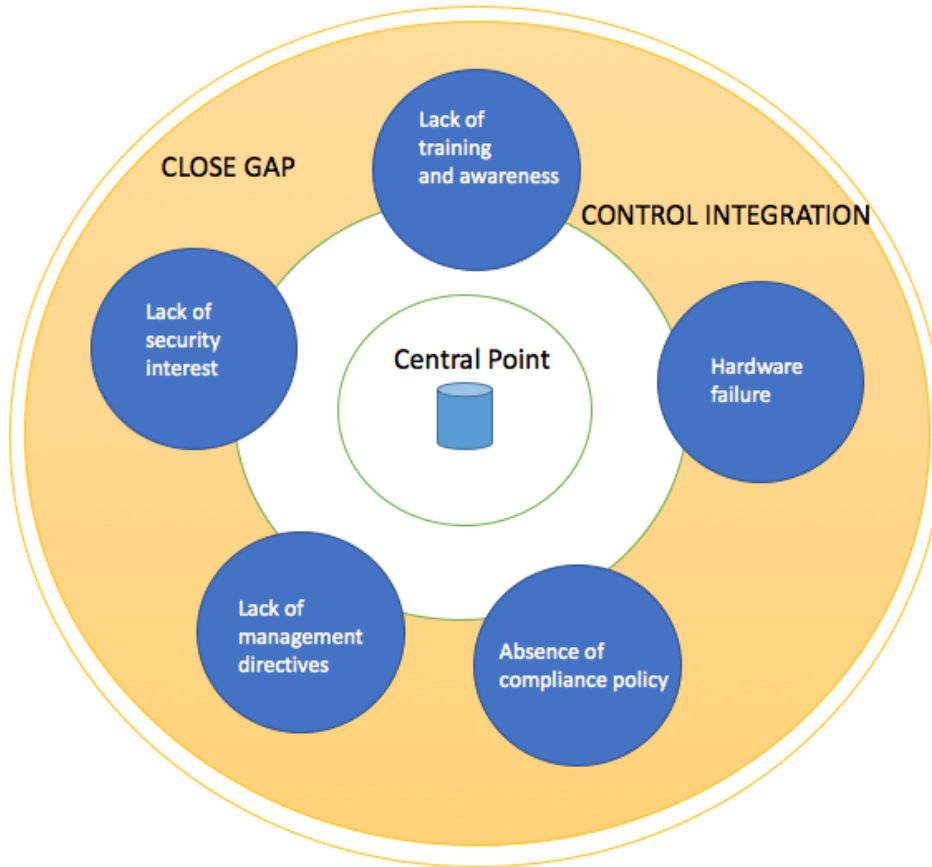


Figure 4. Nine-Five-Circle Model with SPSS Evaluation Results

To ensure that an organization's compliance is established and followed, the NFC principle provides a dynamic compliance process. Here, organizations need to consider that compliance is not a product, but a continuous process that needs to be adjusted frequently to meet administrative constraints and needs. Frequent reassessment will enhance organization activities – especially in the context of security issues, due to the rapid advancement of Information Technology (IT) and increases in its associated risks. Therefore, our proposed principle comes with a dynamic compliance process standard that involves: A) awareness of the compliance regulation; B) controlling integration; and C) closing gaps.

6.2.1. Awareness of compliance regulation

The first step in NFC is to identify the type of governance that will fit in the business domain and then to list any related controls. In this work, we address the five security issues that face the three organizations. As discussed earlier on, the NFC can be scoped to meet individual organization needs; however, for the sake of time, we will address all the three case studies as one example. The first phase

in the NFC principle is to identify metrics that consist of operation, organizing, budgeting, time-frame, managing and reporting procedures. These will enable the management board to utilize that information effectively in the business units, in accordance with regulations and to provide strategic outcomes. From our analysis and findings, the proposed metric consists of the following:

End to end: All members should understand how their efforts contribute to the results. All members need to have a broad understanding of input and output procedures and the effectiveness of the drivers. **Balance:** Here we propose that organizations should incorporate the measurement of their viability and productivity. The utilization of the scorecards will enable organizations to quantify progression status as well as the adequacy of educational programs, occasionally on an alternate cadence than the execution reporting. Lack of security concern is driven by lack of security-awareness training initiatives, and both are due to the absence of policy compliance which is due to lack of management directives and collaboration. Hardware failure could also be seen in this study as being caused by both human and technology factors. Hence it is clear from our SPSS analysis that these factors are interrelated and need to be addressed efficiently for the successful development of ISRM. Furthermore, each of our findings is a critical factor that needs to be addressed efficiently.

f. **Lack of Security Interest, Lack of Security-Awareness Training and Hardware:**

In this study, the three key factors (variables) are related and need to be address first. Here, the organization should develop a formal security awareness team that will be responsible for the development and implementation of a security awareness program. It is also vital that during this phase, each organization has a skilled team, either internally or externally, to maintain this program and all associated hardware. In the NFC, the process of getting the right humans is termed as assembling the security awareness team. The next step in this phase of the NFC is to determine roles for the security awareness program. This is vital in the NFC principle since it enables each organization to train its personnel based on their job functions. This training is extendable, based on subject and area of expertise. Other areas can be joined or removed during this process. The goal here is to develop various levels of in-depth training to enable the organizations to convey the correct training to the perfect individuals at the right time. This approach will enhance each organization's security compliance and the consistency of NFC. Thus, NFC can be applied as a singular approach, or holistic approach, or tiered approach, depending on the organization's prerequisites. One critical point in the phase of selecting the right humans in the NFC is to group individuals by their job functions. In this work, we have

identified three roles, such as “all employees”, “top personnel” and the “management team”. The next phase of the NFC is to apply a tool that can enhance ISRM. It is vital that the proposed programs and hardware are solid for all the groups. In the context of the group “all employees” the proposed program should aim to enable this group to recognize security threats and embrace security as an enhancement tool which is aimed to increase their security interests, and for them to feel comfortable to report those employees creating security risks. The “top personnel” group should concentrate on the employee's commitment to follow security protocols for accessing delicate information and perceive the related dangers if access is abused. The “management” group should comprehend the organization's approach to security and security requirements well enough to examine and strengthen the message to all personnel, encourage personnel security awareness, and perceive and address security-related issues when they arise. As a recommended tool, a “bolt-on tool” can be adopted in this work to enable leaders to have a picture of Service Level Agreement (SLA) performances and have an in-depth view to analyze main causes. The next phase is to develop a fundamental security awareness level for all personnel based on the security awareness program. We recommend security awareness to be transferred either via email, posters, and computer-based training without any restriction in any form. Here we recommend that such security programs should be delivered with regards to the organization culture. This step in the NFC is seen as the development of minimum security awareness. We depict the depth of security awareness training as seen in Figure 5 and illustrate how this stage of the NFC can increase the depth of security awareness and enhance security interest through solid security awareness programs. This process needs to be repeated frequently because in time, the interest of these top managers and other workers deteriorates, and causes such projects also to deteriorate. Furthermore, a classification policy might work during a period of time, but when technology changes, organization also changes as well as the humans. This means old policies will be made obsolete and one cannot comply with an obsolete document.

Up to this stage in our paper, it is clear that the NFC supersedes both the ISO27001 and the ISO27002 because both standards need to be combined to achieve what the NFC has can accomplish. The ISO 27002 provides more details on implementation, but one cannot use it alone as stated in section 6 in this paper because it does not provide any information on which controls need to be implemented, how to measure them and how to assign them to the right

humans. The combination of the two ISO 27000 standards can increase the complexity in the ISRM for companies that are eager to enhance security in a flexible environment. Some organizations can even abuse the ISO 27001 adaptability and concentrate just on the minimum controls with a specific end goal to pass the certification. However, this abuse of the certification process is beyond the scope of this study.

Table 5. SPSS Evaluation Table

SPSS Results	Fintech	Bank	Automobile
Lack of security interest	10%	2%	1%
Lack of security-awareness training	30%	21%	20%
Absence of compliance policy	52%	66%	65%
Lack of Management directives	59%	82%	80%
Hardware failures	55%	1%	2%

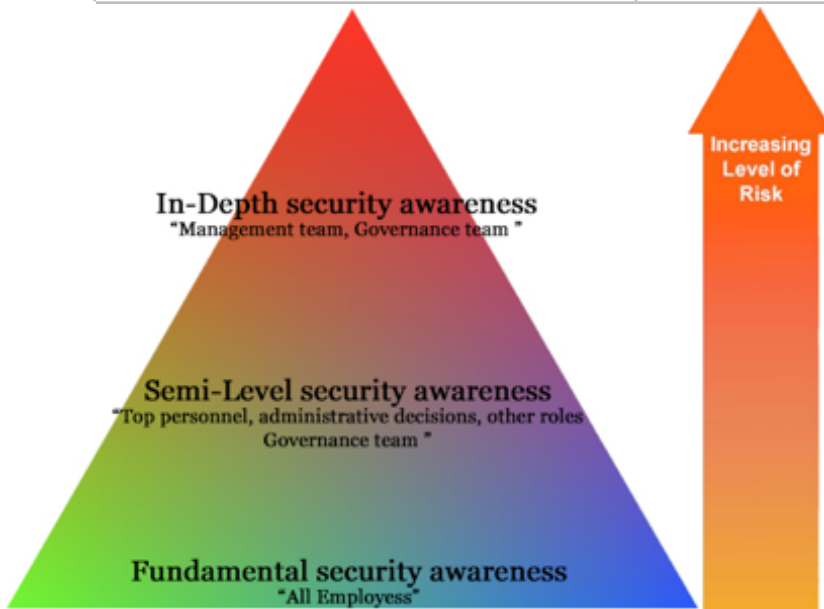


Figure 5. Increasing security interest through a depth security awareness training program

As discussed earlier on, the NFC can be scoped to match an individual organization’s needs. Thus, the training that is held during this phase can be further broken down to map each organizational requirement. For instance, because the percentage of security interest is higher in the FinTech sector than the rest, the FinTech organization could decide on which roles may not need security training in

this phase. This enables each organization to determine the content of training that is needed. Since technological and human factors are interrelated and work together in the NFC principle, a communication channel is needed to deliver security awareness throughout the organization. This is seen as a suitable manner to deliver significant resources to the right humans that fit the organization's interests and culture. As discussed earlier, this form of delivery is not restricted to any communication gateways (hardware and software), but rather, what fits the organization. This flexibility of delivery enhances how employees receive information. However, we recommend that each organization limit its delivery channels so as to enable individuals to remember how information is delivered to them. The communication channel should be made clear to all newly hired personnel and be updated for existing personnel. It is also important in the NFC that both the training content and the communication channel used correspond to each group receiving that particular training. As shown in Figure 6, security awareness needs to be consolidated with other prerequisites located at the central point of the NFC, such as collaboration, culture, confidentiality, integrity, moral agreements, certified skilled leaders, communication, and commitment. Furthermore, because employees react to change in a critical manner, these prerequisites enhance the transparency of the proposed security program and any change that might occur. To guarantee that each group is informed at any point in time when there is a need to occupy a security awareness position, we recommend the organizations add this procedure in their recruiting and re-classifications so that general security awareness training objectives will be actively encouraged without dependence on an individual authoritative unit. Collaboration is characterized as working together with a specific end goal to accomplish an objective. Collaboration comes with participation, commitment, and teamwork. It is seen as a procedure in which at least two humans, groups or organizations, cooperate to achieve shared objectives. The collaboration in information security management enables experts to gather, coordinate, group, disseminate, and share information security know-how with other experts and co-workers. Ahmad et al. (2012) highlighted on the impact of collaboration and communication in the context of information security management. According to Feledi et al. (2013), collaboration involves documentation and scheduling events and can be seen as proposing or submitting, reviewing, commenting and improving knowledge. The organization should also have the right tools to monitor and detect staff activities. For example, accessing violations such as malicious and/or viral software, monitoring unauthorized websites, a tool to monitor and approve the downloading of internet programs and email attachments. Furthermore, other tools to enable productive procedures need to be considered. An example is to enable the organization to assemble, and enhance awareness in performance.

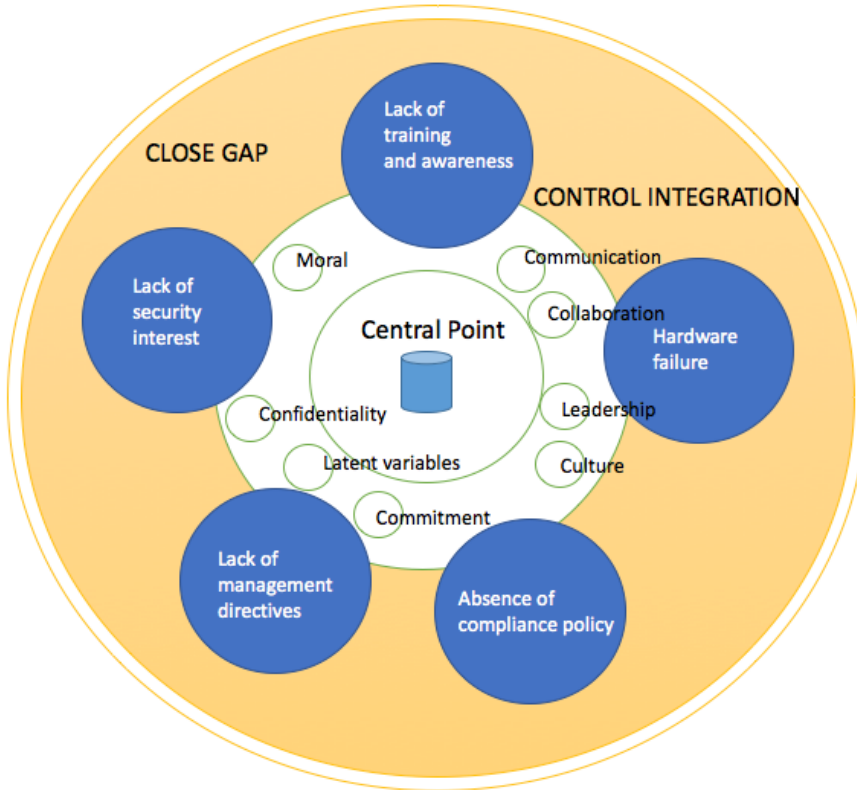


Figure 6. Communication Channels for security awareness training organisation

g. **Lack of Management Directives**

Management leadership and support activity are considered the most critical factors for the security awareness program, and we urge organizations to encourage all personnel to participate and abide by security awareness principles during the life cycle of the NFC. The compliance project should be assigned to a certified leader who has essential abilities. There are several certifications that organizations could look for when deciding on a competent leader such as the CISM, CISSP, Lead ISO 27001 certificate, or the CISA. Here, governing bodies should challenge and question standards at any time, and a responsibility assessment metric should be established to enable an operational team to establish joint decisions frequently. A suitable security awareness method should be established to enforce the security awareness program on the employees. Security metrics should also be added where appropriate, to measure both management and staff performance. The governance team should be proactive and react to any situation by monitoring and measuring progress with deliveries. This is vital for organizations that consolidate procedures and policy and operate globally. All resolved obstructions should be surveyed by the leaders and they should subsequently adjust various

procedure plans into a single cognizant fund plan. Mandates should be established to address the punishment of culprits, security-related guidelines, and the lack of security compliance regulations. We recommend organizations renew the entire process frequently since compliance is not a product, but a continuous process that needs to be adjusted frequently to meet administrative constraints and needs. Frequent assessment will enhance organization activities, especially, in the context of security issues due to the rapid speed of Information Technology (IT) and its associated risks.

6.2.2 Control Integration

The integration phase is where both the control activities and governance targets are defined and institutionalized. Here, the extent to which all the critical factors and latent factors interrelate as well as their main effects are measured. The NFC has the ability to represent unobserved factors or variables in these relationships and account for measurement error in the compliance process. To acquire dependable and predictable result of ISRM development and implementation in the NFC principle, the whole procedure should be controlled and measured persistently. In order to archive that, the complexities of the procedure in terms of different latent variables and interrelated variables need to be separated, comprehended and re-integrated into a point of view to empower complete understanding of the process. The critical issues affecting developing and implementing ISRM need to be identified understood and controlled during the integration. Here procedures such as organizational risk, control targets, testing process, hardware and software tools are all encompassed. This phase enables auditing, identification of non-compliant components and definition of the sources of relationships in governance based on organization risk (Reding et al., 2013). At this level, we can see that the NFC is not prescriptive, but provides organizations with information and tools to make decisions based on their needs – what needs to be done and how to accomplish it. It! is! also a principle that enables organizations to decide on appropriate protections and to take measurement.

6.2.3 Closing Gaps

The absence of compliance in an organization is an indication of poor security measures, causing security risks. Organizations that lack compliance should make sure that decision making includes mechanisms that will enable them to make dynamic decisions and select

mitigating strategies. Lack of information security policy compliance can trigger defective security systems and endanger the business domain. Organizations need to weigh the costs and the risks during mitigation. An advisory board should be set that will advise the IT team regarding the controls needed. Hence, our proposed principle supports our hypothesis in this study that technology and human factors are interrelated and work together for the successful deployment and implementation of information security management in an organization.

7.0. Implications for research, practice and/or society

Our main objective in this study was to address the lack of research evidence on what mobilizes and influences information security management development and implementation. We have fulfilled this objective by surveying, collecting and analyzing data, and by giving an account of the attributes that hinder information security management. Accordingly, a major practical contribution of the present research is the empirical data it provides that enables us to have a bigger picture, and precise information about the real issues that cause information security management shortcomings. Assessing an organization's valuable information will highlight the activities of the CEO, IT managers, top level personnel, policy makers, consultants and trainers to design initiatives, apparatuses and actions in view of what strategy needs to be adopted to implement information security management, what they need to do and where they are now in terms of security-related issues, as opposed to what they think they ought to do. For instance, policy makers could observe that more often than not, top personnel will not read policies specifically and are probably going to pass them to their immediate staff members. This will enable them to reformat their policies accordingly. We believe that, various organizations could derive comparative implications through some of our findings.

Additionally, we believe that our research is especially convenient for several organizations to become more open to challenge and scrutiny. In the event that an organization is having inaccurate idea of their business domain security issues, they may be driven to the idea of applying our NFC principle. This might enable them to develop audit trails of proof in the context of their information systems before making decisions, as opposed to applying standard guidelines which may result in excluding the essential attributes rather than providing them with more prominence attributes, such as, how the employees react to policies, collaboration, communication and commitment. For example, the ISO27001 standard comes with the importance of Statement of Applicability (SoA) while the ISO 9001 comes with the central document that characterizes how an organization should execute a large part of

their information security. This documentation is underrated in the context of NFC because most organizations implementing the ISO 27001 invest more time writing this document than they expected. While this type of information could constitute a critical source of knowledge, the risk is that it is disregarded and not valued enough of the fact that it does not fit the customary formal idea of what constitutes information security management development and have no use in real life.

Furthermore, another essential implication of our study derives from our findings. Our findings indicate a particular set of information sources, capacities, decision strategies, staff and organization attitudes toward security-related issues that can help to close the gap between technology and humans in the context of information security management. Although analyzing the data we collected with a view to distinguishing and systematizing employee skills, behavior, collaboration, commitment, security interest, skilled management directives, technically and frequent security-related issues training goes beyond the remit of this study. We have made contacts with other major firms to explore how this can be accomplished cooperatively in the near future.

Our study is focused on how to nurture and enhance organizations to develop and implement a rigid security policy compliance. Our discoveries recommend in actuality that utilizing flexible tools that can be scoped to meet individual organizational needs have positive effects in the implementation of information security management policies within an organization. Accordingly, our research proposes that organizations should forsake the oversimplified generalized guidelines that neglect the verification of the difference in information security requirements in various organizations. Instead, they should focus on the issue of how to sustain and enhance their organization's compliance through a dynamic compliance process that involves; awareness of the compliance regulation; controlling integration; and closing gaps.

In this sense, despite the fact that our study has limitations concerning the development of a diagnostic tool, it is obviously the main procedure for the measurements of a framework to assess information security compliance policies in the organizations we surveyed. Furthermore, such measurements, which we derived from the SPSS in Figure 2 and Figure 3 subsequently from our NFC in Figure 6 above, recommend that these organizations should reflect on the following questions:

1. What sort of a leadership should be in charge of the Information security management policies?
2. What is the nature of their organization and current information management?
3. What is the nature of their organization security policies at present (e.g., commitment, collaboration, employees' knowledge sharing, humans, technology and how all these factors interrelate and work together).
4. What individual IS principles do they have a tendency to adopt (for example; a principle that can enhance both internal and external environment of the organization IS policies as well as policy compliance operation and strategic)?
5. They also have to assess if they do have the right framework set up (both humans and technology, e.g. employees commitment, collaboration and skilled leadership.) to permit them to establish a rigid policy compliance.

The principle we have graphically demonstrated in Figure 6 can be flexible adopted into any organization and can facilitate vital procedures of developing and implementing rigid information security management policies on the demand of each company over time. The NFC principle likewise recommends that organizations ought to abandon the possibility of general standard ISRM tools that refuse to address the issue of information security management knowledge mobilization in their business domain and focus on tools that can be adjusted to meet the demand of their organization, which in turn, will provide individual and sensitive approaches and solutions in the context of information security management.

7.1. Implications for future research

Our study was based on exploratory and interpretive nature and raises various opportunities for future research, both regarding hypothesis development and idea validation. More research will be important to refine, and advance expounds our discoveries. We do believe that we have generated new findings and useful factors due to the in-depth sampling we obtained from the three organizations we surveyed. However, very little can be said of the nature of data that will be derived from a larger population of bigger firms. Thus, our study could in this manner be extended to analyze a bigger set of statistical data. Furthermore, other research can be conducted to refine and validate our concepts and constructs based on our five key factors derived from the SPSS analyzer. The principle we proposed in this study can also be utilized to create various hypotheses for future empirical testing utilizing a more extensive sample and quantitative research strategies.

Finally, as this study limitation is discussed on section 8, it is therefore essential for further work to be conducted so as to analyze and examine the practices of information security management policies compliance at major firms to explore how this can be accomplished cooperatively in the near future as opposed to the three organizations we surveyed in this study. Additionally, research can in this manner highlight how policy compliance can be conducted across boundaries, such as policy compliance circulation, sharing, and exchange within a firm with several branches in nationwide or across different countries.

8.0. Conclusion and Limitations

Information breaches could be successfully mitigated if security policy compliance is taken seriously in an organization (Ifinedo, 2014; Vance et al., 2012). The arguments of the information security literature and the results from our survey on information security policy compliance via leadership decisions, employee commitment, collaboration and communication have been the main focus of this work. Certain variables such as knowledge sharing, socialization, work experience, skilled leadership management, and intervention can direct employee behaviors toward compliance with information security policies and processes. Sharing information knowledge in an organization enhances both security awareness and the essence of organization security policy compliance and their processes. Leaders in the organization should encourage the importance of knowledge sharing via information security management training, and motivate employees through intrinsic and extrinsic manners for information security risk abatement. Lai and Chen (2014) concur that organization leaders can reward their staff via extrinsic motivation. There is inadequate reward associated with intrinsic motivation because this type of motivation is based on the interest of the employees. Shibchurn and Yan (2015) also added that intrinsic motivations are influenced via satisfaction, and that pleasure is influenced via curiosity.

Based on the results from our three surveys and findings, we have proposed a principle of information security compliance practices based on our proposed NFC principle that enhances information security management by identifying human conduct and IT security-related issues regarding the aspect of information security management. Furthermore, the NFC principle has enabled us to close the gap between technology and humans in this study by proving that the factors in our finding are interrelated and work together, rather than on their own. Therefore, our work presented information security standards and best practices that could be utilized in most business domains. Additionally, we

examined special components and factors that organizations need to be considered when making a decision based on standards.

Despite the fact that our methodology does not convey a new measure, it contributes to a more reliable, good practice of information security measures that help to educate leaders and secure the participation of employees in the context of information security management. The principle quality of our guideline is employees' behavior complexity and related activities. We determined how information security collaboration enhances employee's conduct in the context of complying with policies. Furthermore, we found collaboration as a cooperative approach where different groups of employees work jointly towards the same goal. Leaders can encourage this collaboration via authoritative support and encouragement based on how these leaders reward employees and on how employee well-being matters to the organization (Shropshire et al., 2015).

This study proposes that leaders can encourage security compliance effectiveness by urging employees to share knowledge and collaborate in the context of information security. Sufficient information security management training also has an effect on employee compliance with policies by providing effective IS training courses, frequent workshops, security awareness events, notices, monthly mass-mails, web pages, and frequent meetings. Furthermore, outside events can also enhance IS training procedure in the context of policy compliance process.

Security-awareness training employees in the context of information security management in the right approach sheds light on information security awareness, and adds to the key factors to the success

of information security management in an organization. Another key factor in this research was selecting the right method to support policy compliance implementation. The last key factor is related to the effect of leadership on employee behavior towards policy compliance. Information security "know-how" and "know-why" creates topical mastery for securing information resources in an organization. This engenders a profound understanding of the problems that are associated with poor information security management and throws more lights on policy compliance.

Additionally, we encourage organizations to adopt more encompassing procedures to deal with information security management such as: the interest of leader management; HR management; the implementation and execution of information security policy; IS training; awakening employee security awareness; and group-based decision-making.

We cannot conclude that information security awareness will keep data safe without IS training. Moreover, IS training can enable employees to know why security is important, but this alone will not solve the issues in information security management. This indicates that, without compliance being rigidly established and directed by organization leaders, security-awareness training will not be effective on how humans see information security. Therefore, our work proposes an organization to consider what alternatives there are to enable them to internally and externally communicate security issues with employees. Also, leaders should be trained to manage and direct employees to comply with any policies that governs the organization. We also propose that organizations facing budget constraints and/or time limitations to apply the NFC principle.

References

- A. Hovav, J. D'Arcy. Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the U.S. and South Korea *Inf. Manage.*, 49 (2012), pp. 99–110.
- A. Simmonds, P. Sandilands, L.v. Ekert An ontology for network security attacks S. Manandhar, J. Austin, U. Desai, Y. Oyanagi, A. Talukder (Eds.), *Applied Computing*, Springer, Berlin (2004), pp. 317–323.
- Abawajy J. User preference of cyber security awareness delivery methods. *Behav Inf Technol* 2014;33(3):236–47. doi:10.1080/0144929X.2012.708787.
- Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, 29(4), 432–445.
- Ahmad A, Maynard SB, Park S. Information security strategies: towards an organisational multi-strategy perspective. *J Intell Manuf* 2012;25(2):357–70.
<<http://link.springer.com/10.1007/s10845-012-0683-0>>
- Arachchilage NAG, Love S. Security awareness of computer users: a phishing threat avoidance perspective. *Comput Human Behav* 2014;38(0):304–12. <http://dx.doi.org/10.1016/j.chb.2014.05.046>.

- Ahmad A, Hadgkiss J, Ruighaver AB. Incident response teams – Challenges in supporting the organisational security function. *Comput Secur* 2012;31(5):643–52. doi:10.1016/j.cose.2012.04.001.
- Arce I. The weakest link revisited. *IEEE Secur Priv* 2003;1(2):72–6. Beccaria, C. *On Crime and Punishments*, Bobbs Merrill, Indianapolis, IN. 1963.
- Boss SR, Kirsch LJ, Angermeier I, Shingler RA, Boss RW. If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *Eur J Inf Syst* 2009;18(2):151–64. <<http://www.palgrave-journals.com/doi/10.1057/ejis.2009.8>>; [accessed 16.06.16].
- Breslin, Paul (14 March 2014). "Security updates: The upcoming revision of ISO/IEC 27001". *DNV Business Assurance*. Retrieved 27 January 2015.
- Cavusoglu, H., Cavusoglu, H., Son, J.-Y., and Benbasat, I. 2009. "Information Security Control Resources in Organisations: A Multidimensional View and Their Key Drivers," working paper, Sauder School of Business, University of British Columbia.
- Cavusoglu, H., Mishra, B., and Raghunathan, S. 2004a. "A Model for Evaluating IT Security Investments," *Communications of the ACM* (47:7), pp. 87-92.
- Cavusoglu, H., Mishra, B., and Raghunathan, S. 2004b. "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers," *International Journal of Electronic Commerce* (9:1), pp. 69-104.
- Chang SE, Ho CB. Organisational factors to the effectiveness of implementing information security management. *Ind Manag Data Syst* 2006;106(3):345– 61. <<http://www.emeraldinsight.com/10.1108/02635570610653498>> ; [accessed 08.07.16].
- Chen, Y., Hwang, K., 2006. Collaborative detection and filtering of shrew DDoS attacks using spectral analysis. *J. Parallel Distrib. Comput.* 66, 1137–1151.
- Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M, Baskerville R. Future directions for behavioral information security research. *Comput Secur* 2013;32(0):90–101. <http://dx.doi.org/10.1016/j.cose.2012.09.010>.
- Compston, H. (2009). *Policy Networks and Policy Change: Putting Policy Network Theory to the Test*. Palgrave Macmillan, Basingstoke.

- Da Veiga A, Martins N. Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security* [serial online]. n.d.;49:162-176. Available from: Science Citation Index, Ipswich, MA. Accessed November 28, 2016.
- D.W. Straub, W.D. Nance. Discovering and disciplining computer abuse in organisations: a field study. *MIS Q.*, 14 (1990), pp. 45–60.
- Dhillon, G., and Backhouse, J. 2001. "Current Directions in Information Security Research: Toward Socio-Organisational Perspectives," *Information Systems Journal* (11:2), pp. 127-153.
- Feledi D, Fenz S, Lechner L. Toward web-based information security knowledge sharing. *Inform Secur Tech Rep* 2013;17(4):199–209. <http://dx.doi.org/10.1016/j.istr.2013.03.004>.
- Gaur A. *Statistical methods for practice and research*. SAGE; 2009.
- Guo KH. Security-related behavior in using information systems in the workplace: a review and synthesis. *Comput Secur* 2013;32(1):242–51. < <http://linkinghub.elsevier.com/retrieve/pii/S0167404812001666> > ; Elsevier Ltd.
- Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organisational information security measures. *Information Management & Computer Security*, 16(4), 377–397.
- Hair JF, Black WC, Babin BJ, Anderson RE, editors. *Multivariate data analysis*. 7th ed. 2010.
- Harrison K, White G. An empirical study on the effectiveness of common security measures. *Proc 43rd Hawaii Int Conf Syst Sci*. Koloa, HI, 1–9. < <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5428509> > ; 2010 [accessed 24.06.16].
- Herath, T., and Rao, H. G. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 106-125.
- Herath T, Rao HR. Encouraging information security behaviors in organisations: role of penalties, pressures and perceived effectiveness. *Decis Support Syst* 2009a;47(2):154–65. < <http://linkinghub.elsevier.com/retrieve/pii/S0167923609000530> > ; [accessed 13.05.16].

- Herbert, Chantall (3 June 2014). "More changes ahead. ISO 27001:2005 Information Security Management Standard". QSL. Retrieved 27 January 2015.
- Hsu CW. Frame misalignment: interpreting the implementation of information systems security certification in an organisation. *Eur J Inf Syst* 2009;18(2):140–50. <<http://www.palgrave-journals.com/doi/10.1057/ejis.2009.7> > ; [accessed 03.07.16].
- Hsu CW, Lee J-N, Straub DW. Institutional influences on information systems security innovations. *Inf Syst Res* 2012;23(3-Pt -2):918–39. <<http://isr.journal.informs.org/cgi/doi/10.1287/isre.1110.0393> >.
- Hu Q, Hart PJ, Cooke D. The role of external and internal influences on information systems security: a neo-institutional perspective. *J Strateg Inf Syst* 2007;16(2):153–72. <<http://linkinghub.elsevier.com/retrieve/pii/S0963868707000212> > .
- Ifinedo P. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. *Comput Secur* 2012;31(1):83–95. <http://dx.doi.org/10.1016/j.cose.2011.10.007>.
- Ifinedo, P. and Olsen D (2014). An Empirical Research on the Impacts of Organisational Decisions' Locus, Tasks Structure Rules, Knowledge, and IT Function's Value on ERP System Success, *International Journal of Production Research*, 53, 8. DOI: 10.1080/00207543.2014.991047 [ISSN 0020-7543 (Print), 1366-588X (<http://faculty.cbu.ca/pifinedo/IJPRDR.pdf>)].
- J.-Y. Son. Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Inf. Manage.*, 48 (2011), pp. 296– 302.
- Jaeger, J. (2013). Human error, not hackers, cause most data breaches. *Compliance Week*, 10(110), 56–57.
- Jansson K, von Solms R. Phishing for phishing awareness. *Behav Inf Technol* 2013;32(6):584–93.
- Joshi, K. 2005. "Understanding User Resistance and Acceptance During the Implementation of an Order Management System: A Case Study Using the Equity Implementation Model," *Journal of Information Technology Case and Application Research* (7:1), pp. 6-20.
- K.H. Guo, Y. Yuan. The effects of multilevel sanctions on information security violations: a mediating model *Inf. Manage.*, 49 (2012), pp. 320-326.

- K. Siau, F.F.-H. Nah, L. Teng. Acceptable internet use policy. *CACM*, 45 (2002), pp. 75–79
- Kankanhalli, A., Teo, H.-H., Tan, B. C., and Wei, K.-K. 2003. "An Integrative Study of Information Systems Security Effectiveness," *International Journal of Information Management* (23:2), pp. 139- 154.
- Kim, H. W., and Pan, S. L. 2006. "Towards a Process Model of Information Systems Implementation: The Case of Customer Relationship Management (CRM)," *Data Base for Advances in Information Systems* (37:1), pp. 59-76.
- Kurt F. Reding, Paul J. Sobel, Urton L. Anderson, Michael J. Head, Sridhar Ramamoorti, Mark Salamasick, Cris Riddle (2013), "Internal Auditing: Assurance & Advisory Services".
- Kritzinger E, von Solms SH. Cyber security for home users: a new way of protection through awareness enforcement. *Comput Secur* 2010;29(8):840–7. <http://dx.doi.org/10.1016/j.cose.2010.08.001>.
- Lee, J., and Lee, Y. 2002. "A Holistic Model of Computer Abuse Within Organisations," *Information Management and Computer Security* (10:2/3), pp. 57-63
- Li H, Zhang J, Sarathy R. Understanding compliance with internet use policy from the perspective of rational choice theory. *Decis Support Syst* 2010;48(4):635–45. <http://dx.doi.org/10.1016/j.dss.2009.12.005>.
- J, Li N, Wang X, Yu T. Denial of service Li attacks and defences in decentralised trust management. *International Journal of Information Security* 2009;8:89e101.
- Loster, P. C. (2005). Managing e-business risk to mitigate loss. *Financial Executive*, 21(5), 43–45.
- M.d. Vivo, G.O.d. Vivo, G. Isern. Internet security attacks at the basic levels *ACM SIGOPS Oper. Syst. Rev.*, 32 (1998), pp. 4–15
- Ma, Q., Schmidt, M. B., & Pearson, J. M. (2009). An integrated framework for information security management. *Review of Business*, 30(1), 58–69.
- Mackie, Ryan (2 April 2013). "ISO 27001:2013 – Understanding the New Standard". *The Pragmatic Auditor*. Retrieved 27 June 2016.
- McFadzean E, Ezingear J-N, Birchall D. Anchoring information security governance research: sociological groundings and future directions. *J Inf Syst Secur* 2006;2(3):3–48.

- McFadzean E, Ezingear J-N, Birchall D. Information assurance and corporate strategy: a Delphi study of choices, challenges, and developments for the future. *Inf Syst Manag* 2011;28(2):102–29. <
<http://www.tandfonline.com/doi/abs/10.1080/10580530.2011.562127> >; [accessed 15.06.16]
- Mirkovic, J., Reiher, P., 2005. D-WARD: a source- end defense against flooding denial-of-service attacks. *IEEE Trans. Dependable Secure Comput.* 2, 216–232.
- Pahnila, S., Siponen, M., and Mahmood, A. 2007. “Employees’ Behavior towards IS Security Policy Compliance,” in *Proceedings of the 40th Hawaii International Conference on System Sciences*, Los Alamitos, CA: IEEE Computer Society Press, pp. 156-166.
- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS- Q). *Computers & Security*, 42, 165–176.
- PricewaterhouseCoopers. 2008. “Employee Behaviour Key to Improving Information Security, New Survey Finds,” June 23, (<http://www.ukmediacentre.pwc.com/content/detail.aspx?releaseid=2672&newsareaid=2>).
- Puhakainen, P., & Siponen, M. (2010). Improving employees’ compliance through information systems security training: an action research study. *Mis Quarterly*, 34(4), 757–778.
- Rubenstein, S., & Francis, T. (2008). Are your medical records at risk? *Wall Street Journal—Eastern Edition*, 251(100), D1–D2.
- S.J. Harrington. The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Q.*, 20 (1996), pp. 257– 278.
- Safa NS, Sookhak M, Von Solms R, Furnell S, Ghani NA, Herawan T. Information security conscious care behaviour formation in organisations. *Comput Secur* 2015;53(0):65–78.
<http://dx.doi.org/10.1016/j.cose.2015.05.012>.
- Schultz EE, Proctor RW, Lien M-C, Salvendy G. Usability and security an appraisal of usability issues in information security methods. *Comput Secur* 2001;20(7):620–34.
- Schumacker RE, Lomax RG. A beginner’s guide to structural equation modeling. 3rd ed. New York: Taylor & Francis Group; 2010.

- Seo, D., Lee, H., Perrig, A., 2013. APFS: adaptive probabilistic filter scheduling against distributed denial-of-service attacks. *Comput. Secur.* (In Press).
- A.N. Singh, A. Picot, J. Kranz, M.P. Gupta, A. Ojha. Information security management (ISM) practices: lessons from select cases from India and Germany *Global Journal of Flexible Systems Management*, 14 (4) (2013), pp. 225–239
<http://dx.doi.org.ezproxy.derby.ac.uk/10.1007/s40171-013-0047-4>.
- Siponen, M. T. 2005. "An Analysis of the Traditional IS Security Approaches: Implications for Research and Practice," *European Journal of Information Systems* (14:3), pp. 303-315.
- Siponen, M., and Vartiainen, T. Unauthorized copying of software and levels of moral development: A literature analysis and its implications for research and practice. *Information Systems Journal*, 14, 4 (2004), 387 - 407.
- Siponen, M., Mahmood, M. A., & Pahlila, S. (2014). Employees' adherence to information security policies: an exploratory field study. *Information & Management*, 51(2), 217–224.
- Soo Hoo, K. J. 2000. "How Much Is Enough: A Risk Management Approach to Computer Security," working paper, Center for International Security and Cooperation, Stanford University (available online at http://cisac.stanford.edu/publications/how_much_is_enough__a_riskmanagement_approach_to_computer_security/).
- Straub, D. W., and Nance, W. D. 1990. "Discovering and Disciplining Computer Abuse in Organisations: A Field Study," *MIS Quarterly* (14:1), pp. 45-60.
- T.P. Cronan, C.B. Foltz, T.W. Jones. Piracy, computer crime, and IS misuse at the university. *CACM*, 49 (2006), pp. 84–90
- Trcek, D., Trobec, R., Pavesic, N., & Tasic, J. F. (2007). Information systems security and human behaviour. *Behaviour & Information Technology*, 26(2),113–118.
- V.K.G. Lim, T.S.H. Teo. Prevalence, perceived seriousness, justification and regulation of cyberloafing in Singapore: an exploratory study. *Inf. Manage.*, 42 (2005), pp. 1081–1093.
- Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*, 29(4), 263–290.

- Yeniman, Y., Ebru Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing information security management in small-and medium-sized enterprises: a case study from turkey. *International Journal of Information Management*, 31(4), 360–365.
- Wang, H., Jin, C., Shin, K.G., 2007. Defense against spoofed IP traffic using hop-count filtering. *IEEE/ACM Trans. Netw.* 15, 40–53.
- Webb J, Ahmad A, Maynard SB, Shanks G. A situation awareness model for information security risk management. *Comput Secur* 2014;44(0):1–15. <http://dx.doi.org/10.1016/j.cose.2014.04.005>.
- Werlinger R, Hawkey K, Beznosov K. An integrated view of human, organisational, and technological challenges of IT security management. *Inf Manag Comput Secur* 2009;17(1):4–19. <<http://www.emeraldinsight.com/10.1108/09685220910944722>>; [accessed 13.06.16].
- Werlinger R, Hawkey K, Botta D, Beznosov K. Security practitioners in context: their activities and interactions with other stakeholders within organisations. *Int J Hum Comput Stud* 2009;67(7):584–606. <http://dx.doi.org/10.1016/j.ijhcs.2009.03.002>.
- Willison, R. 2006. “Understanding the Perpetration of Employee Computer Crime in the Organisational Context,” *Information and Organisation* (16:4), pp. 304-324.
- Witherspoon CL, Bergner J, Cockrell C, Stone DN. Antecedents of organisational knowledge sharing: a meta-analysis and critique. *J Knowl Manag* 2013;17(2):250–77. doi:10.1108/13673271311315204.
- Y. Chen, D.L. Nazareth, K.-W. Wen. Research in information security: a literature review using a multidimensional framework *Proceedings of the Thirty-Ninth Annual Western Decision Sciences Institute Conference (WDSI 2010), Lake Tahoe, NV (2010)*, pp. 3681–3687.
- Y. Lee, K.A. Kozar. An empirical investigation of anti-spyware software adoption: a multitheoretical perspective. *Inf. Manage.*, 45 (2008), pp. 109–119.
- Zhang J, Reithel BJ, Li H. Impact of perceived technical protection on security behaviors. *Inf Manag Comput Secur* 2009;17(4):330–40.

Conclusion to STUDY 5: Information security management and the human aspect in organisations

Across all the organisations studied in papers 1, 2, 3 and 4, the fifth study focused on the process of developing and implementing an effective information security management system. The results of the study indicate that organisations will continue to be exposed to cyber threats that damage their reputation and cost them a lot of money if management measures are not taken to ensure that information systems are carefully implemented and managed.

The research included a comprehensive analysis of the human aspects influencing the general effectiveness or ineffectiveness of current security systems, especially the responsible attitude that senior management and staff members have toward information security. The impact of cross-functional involvement on a target group was also extensively examined in the research. In other words, the overall effectiveness of security measures for digital strategies is increased by security strategies that incorporate the entire organisation. Particularly in the case of executive support and involvement (Parsons, McCormac, Butavicius, & Ferguson, 2010).

The development of a strict information security policy was a further crucial component (Ifinedo, 2014; Vance et al., 2012; Stewart, 2022). In this study, the information security policy compliance through leadership decisions, employee involvement, collaboration, and communication were taken into consideration along with the justifications from the information security literature and the survey results. The methodology used in paper 5 has contributed to a more reliable, well-established practice of information security measures that contribute to the security of the IS. This paper suggested that managers proactively ensure security compliance through encouraging their employees to share knowledge and collaborate in the area of information security. In addition, training employees on information security management in the right approach enlightens information security awareness and contributes to the key factors for the success of information security management in an organisation. The results also indicated that sufficient information security management training can influence staff information ISP compliance.

The paper urged organisations to adopt more thorough approaches to information security management, including executive level interest, human resource management, information security policy implementation and execution, information security training, employee security awareness and group-based decision-making.

The paper encouraged organisations to adopt more encompassing procedures to deal with information security management such as: the interest of leader management; HR management; the implementation and execution of information security policy; IS training; awakening employee security awareness; and collective-based policymaking.

In order to strengthen the role of the information security policy in cybersecurity, the question arises as to which level and which comprehensive approach an organisation should adopt. This is an extremely important question because there is no one-size-fits-all solution and the answers in the literature are inadequate because they lack the holistic approach needed to develop a successful ISP and achieve compliance.

In order to integrate many components in a thorough manner and enhance ISP development and compliance in a multinational firm, Research 6 suggests a study model based on the NFC model. The practicality of the NFC model has been demonstrated and the action research methodology used for validation produced encouraging results.

Chapter 9. STUDY 6: A systematic framework to explore the determinants of information security policy development and outcomes:

Introduction

This study builds upon the previous five studies and aims to establish a framework for creating an effective information security policy (ISP) using the data collected. ISPs are crucial in today's business world, but the risk of cyber threats increases when employees fail to comply. Therefore, it is necessary to implement management strategies to ensure ISP compliance, as failure to do so can damage an organization's reputation and result in significant financial losses. The paper's author, Harrison Stewart, outlines his contributions, detailed on the following page.

<https://doi.org/10.1108/ICS-06-2021-0076>

Statement of Authorship

CO-AUTHORSHIP APPROVALS FOR HDR THESIS EXAMINATION

PUBLICATION 6

This section is to be completed by the student and co-authors. If there are more than four co-authors (student plus 3 others), only the three co-authors with the most significant contributions are required to sign below.

Please note: A copy of this page will be provided to the Examiners.

Full Publication Details	A systematic framework to explore the determinants of information security policy development and outcomes Stewart, H. (2022), "A systematic framework to explore the determinants of information security policy development and outcomes", Information and Computer Security, Vol. 30 No. 4, pp. 490-516. https://doi.org/10.1108/ICS-06-2021-0076									
Section of thesis where publication is referred to	All									
Student's contribution to the publication	<table style="width: 100%; border: none;"> <tr> <td style="text-align: center; border-bottom: 1px solid black; width: 10%;">100</td> <td style="text-align: center; width: 5%;">%</td> <td style="width: 80%;">Research design</td> </tr> <tr> <td style="text-align: center; border-bottom: 1px solid black;">100</td> <td style="text-align: center;">%</td> <td>Data collection and analysis</td> </tr> <tr> <td style="text-align: center; border-bottom: 1px solid black;">100</td> <td style="text-align: center;">%</td> <td>Writing and editing</td> </tr> </table>	100	%	Research design	100	%	Data collection and analysis	100	%	Writing and editing
100	%	Research design								
100	%	Data collection and analysis								
100	%	Writing and editing								

Outline your (the student's) contribution to the publication:

Harrison Stewart is the sole owner of this publication.

APPROVALS

By signing the section below, you confirm that the details above are an accurate record of the students contribution to the work.

Name of Co-Author 1 _____ Signed _____ Date _____

Name of Co-Author 2 _____ Signed _____ Date _____

STUDY 6

A systematic framework to explore the determinants of information security policy development and outcomes

Harrison Stewart

Abstract

The current complexity of cyber threats and organisational complexity requires ISP development to take a more holistic approach than the incomplete approach. Previous frameworks have been proposed to improve the role of information security policy in information security management. However, they all fall short because they lack the holistic approach needed to develop a successful ISP and achieve compliance. This study proposes a research model based on the Nine-Five-Circle (NFC) framework that aims to combine six constructs, latent variables, and factors from previous research models in a holistic manner to improve ISP development and compliance in a multinational organisation research approach used to validate the NFC model provided positive results and its feasibility for practical use was confirmed.

Keywords – ISP Development, Information Security Procedure, Nine-Five-circle (NFC), Information Systems Security, Information Security Commitment

Paper type - Research paper

1.0. Introduction

There are several definitions for an ISP in the literature. The ISP is a governing document that defines the overall boundaries of information security in an organisation (Sohrabi et al., 2016; Lucila, 2016). It also demonstrates management's commitment to and support for information security in an organisation and the role it plays in achieving and supporting the organisation's vision and purpose (Sohrabi et al., 2016; Knapp et al., 2009; Kadam, 2007; Lucila, 2016). Management endorsement,

relevance to the organisation in question, practicality, achievability, flexibility and enforcement, and the fact that the policy includes all relevant parties are all aspects that contribute to a successful ISP.

Information technology (IT) is of great importance to organisations as it facilitates daily operations and various mission-critical operations, and therefore an ISP is a necessity for business continuity. To achieve ISP objectives, a robust security framework must ensure confidentiality, integrity, availability, authenticity, authority, verifiability, and non-repudiation of critical information assets (Alhanahnah et al., 2016).

The ISP formulates the attitude of the organisation towards information assets that must be secured from unauthorised access, exposure, corruption and alteration (Mauritian, 2011). Formulation policies are typically adopted to monitor the exposure and misuse of information. International templates for security policies that are available should be considered as a preparatory tool for policy development purposes (Goel & Chengalur, 2010; Baskerville & Siponen, 2002). According to (Waddel, 2013), developing a security strategy is lengthy, challenging as well as costly. This assertion has also been supported by (Goel & Chengalur, 2010). Replication of an ISP from another entity may be insufficient to address specific concerns such as ISP programs with existing rules and regulations. Even a well-replicated policy may be insufficient under certain circumstances (Bjorck, 2004; Kusserow, 2014), and therefore ISP strategies should be defined based on the organisation's culture, beliefs, operations, environment, and policy requirements (Siponen & Willison, 2009; D'Arcy et al., 2009). By considering different types of facilities, users and management support, technological changes, social concerns, cultures, economic, legal and political when formulating and developing ISPs (Goel & Chengalur, 2010).

Regardless of how robust and sophisticated the technologies are today to ensure information security, human factors are still considered the weak link in the security chain (Stewart, 2020). Human factors have been the subject of extensive research, which has concluded that employee threats are among the greatest threats to information security in the last decade (Mattord, Levy & Furnell, 2014).

Cybersecurity Insider's reports that 64% of insider threats go unchecked or undetected, and Forrester predicts that insider threats will increase 8% by 2021 (Forrester, 2021). Yahoo! reported a breach of 1.5 billion user accounts caused by insiders, and a study conducted found that insiders are responsible for a quarter of all data breaches worldwide (Singh Lodhi & Kaul, 2016) and insider attacks cause more damage than outsider attacks (Gelles, 2016). Most of these insider threats are associated with either ill-defined ISP or lack of ISP. Eloff & Eloff (2005) proposed that all aspects of information security must be addressed in a well-structured and holistic manner to prevent security breaches. Several suggestions

have been made regarding two elements to consider in developing a well-defined ISP, namely the development process (Tuyikeze & Flowerday, 2014; Flowerday & Tuyikeze, 2016; Lucila, 2016) and the content of the ISP (Doherty et al., 2011; Maynard & Ruighaver, 2006). Additionally, an effective ISP ought to convert the expectations of management into well-defined, measurable and distinct objectives, and demonstrate its validity, legibility and sustainability (Goel & Chengalur, 2010).

Several papers have focused more on the structure and content of the ISP (Tuyikeze & Flowerday, 2016; Lucila, 2016), while less attention has been paid to the development of the process, particularly the step-by-step process for developing a strategic ISP for a multinational company discussed in this paper. This study highlights factors required to justify and establish an ISP based on the needs of an organisation and relevant regulations and laws (Wiander, 2009). Many security experts also share the opinion that the implementation and enforcement of security policies represent one of the most practical methods of maintaining and protecting information systems, being also one of the keys to a successful security control programme (Knapp et al., 2009; Sohrabi et al., 2016). Yet, in developing an effective ISP, two elements in ISP that impact its efficacy are the development process and the content (Flowerday & Tuyikeze, 2016; Tuyikeze & Flowerday, 2014; Lucila, 2016; Stewart, 2020). Improving existing practice is important to the quality of strategic ISPs. In other words, it examines how organisations create, implement, utilize, and maintain strategic security policies and attempts to alter organisational practice in order to enhance the overall quality of the policies that arise. As with many organisational efforts, the behavior and attitudes of individuals participating have an impact. Furthermore, acknowledging that various stakeholders will have varying perceptions of quality and allowing for the correction of these perceptions will be essential in enhancing ISP development. This study focuses on ISP development in an organisation.

This paper is organized as follows: First, an overview of this work is provided. Then, the challenges related to the development of information security and the case study for this work are presented. Then, the steps of NFC are discussed and how they were used in this work to answer the research question. Followed by ISP success factors and discussions. Finally, the implications for research are highlighted and the value of our findings to practitioners is discussed.

2.0. Literature Review

There are several approaches to policy development and formulation today. Table 1 sums up the concepts and ideas of various writers on ISP development techniques and procedures.

Table. 1 A Review of the ISP Development Literature

No.	Author	Paper contribution
1	Lucila, N. B. (2016)	A literature review conducted revealed that there are a limited number of frameworks and models for ISP development and that current models are limited in terms of empirical research.
2	Flowerday, S. V., Tuyikeze, T. (2016)	Suggested information security governance framework should be conducted at all levels of management, namely: strategic, tactical, and operational, and each policy within each of these levels should be outlined within the ISP architecture (ISPA) of an organisation.
3	Soomro, Z. A., Shah, M. H., and Ahmed, J. (2016)	Suggest that organisations should take a more holistic approach to information security management that includes all aspects of organisation such as executive, human resource management, policy makers, decision makers and information security training awareness.
4	Sohrabi, N., Von Solms, R., Furnell, S., Elizabeth, P., and Africa, S. (2016)	The results of the data analysis revealed that information security, knowledge sharing, collaboration, intervention and experience all have a significant effect on employees' attitude towards compliance with organisational ISPs.
5	Hallsworth, R. M., and Parker, S. (2015)	Suggest that policy reformation success lies upon an effective partnership between civil servants and ministers.

6	Ifinedo, P. (2014)	Suggests that employees' control beliefs, skills, and competencies related to information systems security also influence their intention to comply with the ISSP.
7	Waddell, S. A. (2013)	The study uses content analysis and cross-case analysis methods to identify challenges in ISP development. It suggests further investigation of specific development processes, such as the Acceptable Use Policy or a specific system ISP.
8	Tuyikeze, T., and Flowerday, S. (2014)	Suggest various factors that a given organisation must consider in developing and implementing ISP.

There is a consensus in the literature that developing an effective ISP requires a holistic view, and therefore the current literature lacks a comprehensive methodology or mechanism for developing ISP. This suggests that a more pragmatic strategy for developing, implementing, and applying an effective ISP is needed, which is addressed in this paper.

3. THEORETICAL BACKGROUND FOR DEVELOPING THE PROPOSED FRAMEWORK IN RELATION TO ISP

The NFC has less academic review since the concept is new, however it does fit this work and should help us identify the needs for implementing operational and ISP improvements. It should also enable us to focus on ISP measurement, assessing organisational ISP performance, employees information security awareness and improving the interrelationship between information security and humans.

This paper uses the NFC technique to find the solution of the questions raised in this paper. Stewart (2020; 2021) defines NFC as an information security framework or approach that identifies the imperatives for implementing operational and information security improvements. It also places more emphasis on measuring and evaluating an organisation's ISP performance and outsourcing, as well as improving the interrelationship between technology and human factors. Having mentioned that NFC is the right technique for this work, this work must follow a well-structured process to ensure reliability and validity. Stewart & Jürjens (2017) highlight three steps that should be followed when using NFC. These are (i) situational awareness, (ii) integrational control, and (iii) gap-closure. Situational awareness defines the problem and its possible causes. The integrational control is the execution, controlling and the assessment phase, while the gap-closure includes the measures necessary to ensure

that the entire process is completed at a satisfactory level and that the process follows the standards set out in the organisation's ISP.

Situational awareness focuses on analysing the organisational security situation and helps derive appropriate constructs and latent variables needed to address the problem at hand. The integrative control of the NFC framework includes constructs and other latent variables derived based on organisational situational awareness. The approach involves segmenting each construct into its respective topology as shown in Figure 1. Each of the three steps of the NFC is discussed on how it has been applied in this research paper.

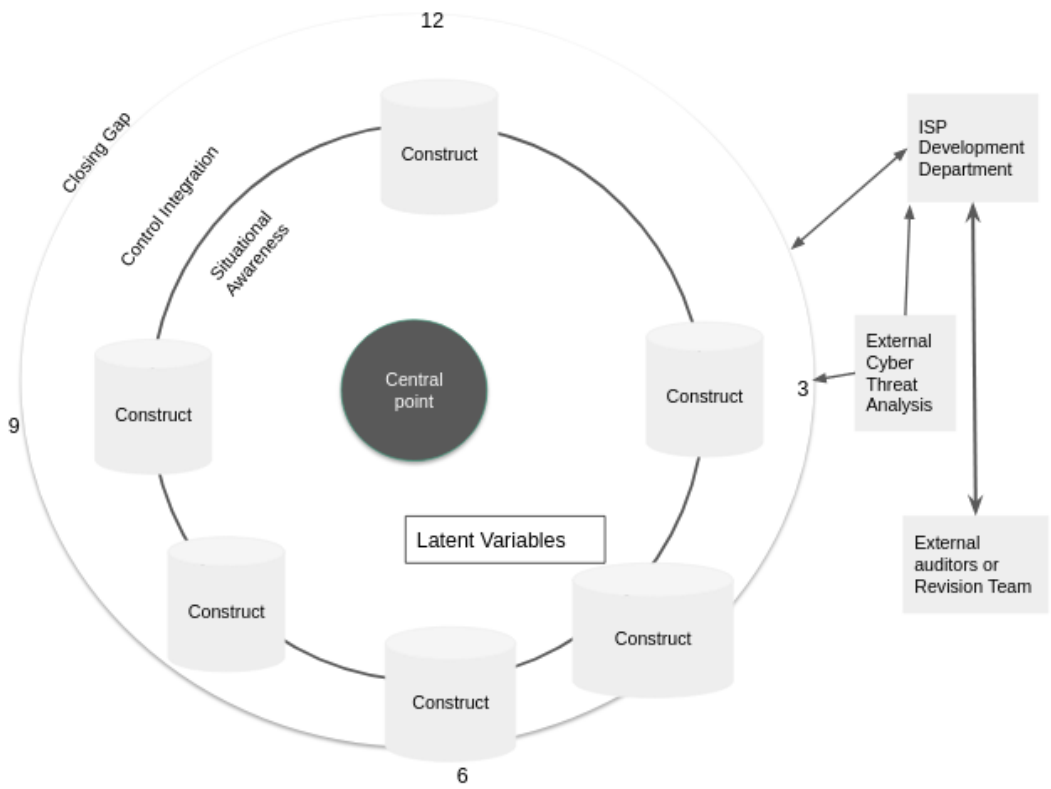


Figure 1. NFC Framework

According to Stewart & Jürjens, the key constructs are encapsulated in the control integration and gap closure dynamics. These constructs are the underlying key factors on which this work is based and are derived through data collection and analysis. According to (Stewart & Jürjens, 2017), the NFC concept is also based on a rotation-driven approach using the central point as shown in Figure 1, and the minimum number of rotations is five times in each life-cycle to ensure stabilization of the process. The rotation starts at the 9 o'clock, 12 o'clock, 3 o'clock, 5 o'clock, 6 o'clock, and 7 o'clock positions.

During each cycle, organisations can adjust the constructs to meet their needs. The stabilization process is often referred to as the SDCA (standardize-do-check-action) cycle. Besides the “central point” as shown in Figure 1 are latent variables considered as the choices that can be made based on the decisions of the organisation to implement the ISP. On the other side of NFC are other components, namely the ISP development department, the ISP facilitators, white/black box testing, and regulatory or IT audits.

The IS Policy Department defines and determines the motivation behind the process and establishes policies that address rules and regulations within the ISP and between it and the rest of the organisation;

White/black box testing and external audits examine ISP to ensure that the specific ISP implemented improves the knowledge domain, the types of practices the ISP addresses, and existing knowledge management processes; including benefits, costs, and relevant services; and the technology aspect, which relates to the role of enabling technologies. The audit is conducted at regular intervals to determine the maturity level of the project. According to Ishikawa (1985), “Failure to revise standards and regulations is proof that no one is seriously using them.” Each construct in the work is analyzed and prioritized by measuring the impacts against the probability during each lifecycle.

The facilitators take on the role and responsibility of guiding the ISP project team through a clearly defined sequence of activities that maps the progress of the ISP project from initiation to completion.

4.0. Research Methodology

The formal content analysis of current theories and techniques for establishing an ISP was conducted using a qualitative methodology in this study. The interpretation of the content analysis results led to the development of a conceptual framework. Furthermore, in order to generalize the results, a survey was conducted to collect data to validate the constructs contained in the proposed framework (Component 1 in Figure 2).

4.1. Content Analysis

In order to get a full knowledge of the procedures required to create ISP, a content analysis method of ISP was highly reliant on the coding procedure. The basic coding approach in content analysis attempts to arrange massive amounts of text into many fewer topic categories. To gain a comprehensive knowledge of the procedures required to develop an ISP, a content analysis of ISP development was conducted using secondary sources in the literature. As indicated in Table 1, a total of 9 documents were chosen for this study's sample. The qualitative research tool HyperRESEARCH was used to analyze all the 9 documents. All documents were classified separately by emphasizing the wording describing the process of creating an ISP. Following the completion of the coding procedure, a total of 23 codes and 135 cumulative codes were obtained. These codes ranged from the general to the particular. Common codes consisted of 'ISP purpose and objectives,' whereas detailed codes included 'drafting the ISP,' 'writing the ISP,' and 'ISP process.'

The total of 23 codes discovered during the coding process were reduced to 6 (see Fig. 2), while some of the smaller codes were combined with comparable, related codes. For instance, the codes "security awareness", "threat detection" and "threat protection" were grouped under one code called "cbyer threat intelligence", as they are all part of the security risk process assessment. A conceptual framework was created based on the findings of the content analysis. The suggested framework was then fine-tuned based on feedback from the experts who were surveyed.



Figure 2. Framework codes resulted from the content analysis

4.2. Data Collection

The major source of data for this study was a survey that was performed to validate the structures of the framework's NFC component. A questionnaire was created and sent to 40 security specialists, managers, stakeholders, and all leaders. Following best practices in developing the questionnaire, the objectives of the survey, the resources, the budget and the deadlines were determined by the management and the researchers (Umbach, 2004). The methods for conducting the survey were online survey, postal survey, telephone survey and face-to-face survey (Witmer et al., 1999; Myers and Newman 2007; Walsham 2006). These methods were agreed upon by the researchers and management due to their benefits and drawbacks. After this phase, the question format was determined, which consisted of both open and closed questions (Neuman, 2007). Closed questions on a Likert scale were also included in the survey, requiring respondents to choose from a predetermined selection of options. The flow of the questions was then designed to ensure the logical flow of the

questions by avoiding responses from unqualified respondents (Sax et al., 2003) to ensure that respondents were comfortable to provide honest answers (Myers and Newman 2007; Walsham 2006). The questionnaires were divided into five parts: (i) introduction (ii) preliminary screening of respondents (iii) welcome questions (iv) progression to more detailed and difficult questions and (v) closure. The questionnaires were then assessed to determine whether they were necessary, how long they were, and if they provided all of the information needed for this study. Following client acceptance, the researcher pretested and amended the questionnaire, resulting in the final layout of the questionnaire for client approval. After the final copy and layout of the questionnaire had been approved, it was time to field the questionnaire, i.e., conduct the survey.

The questionnaire, which was produced using Cetbix Survey software, received 30 responses from the experts. The participants were chosen because they work with information security issues on a daily basis and so have a major effect on the development of information security in an organisation. The data analysis was conducted using the SPSS program. The pilot test in the initial phase consisted of 95 questions. In the final version, based on feedback from the pilot test, there were 44 questions. During the pilot test, a select group of employees tried out the 95 questions being tested and provided their feedback before the final questions were fully deployed. The interviews lasted 60 minutes. All questions surveyed related to an item shown in Table 2. Subsequently, semi-structured interviews were conducted to gain a deeper understanding of employees' perceptions and opinions of ISP, particularly in relation to their current practices and their ability to use their current ISP. During the interview, open-ended questionnaires were used (Britten, 1995). The interview began with questions that participants could easily answer and then progressed to more difficult and sensitive topics. This helps to make respondents feel comfortable, build trust and rapport (Stewart & Jürjens 2018), and generate rich data with which to subsequently develop the interview (Britten, 1999). The data collection phase was conducted with the direct participation of the employees, and the ISP program manager. All questions surveyed related to an item shown in Table 2.

Table 2. Questionnaire and related items

Related Items	Questions
General Questions	Q1- Q9
Management & Oversight	Q10- Q19
Data Security	Q20 - Q22

Employee Security Awareness	Q23- Q28
Cybersecurity Intelligence	Q29 - Q35
ISP Questions	Q36 - Q44

The questionnaires were based on different industry standards that seemed well suited for this work and were tailored to the specific needs of the organisation. In addition, part of the questionnaire was also based on the results of the content analysis. The tailoring of the questionnaire helped to get a clear picture of the organisation's data security measures. Respondents were invited to offer any ideas they had for improving the procedures for establishing and executing an ISP that were not included in the questionnaire. Systematic sampling was used to select respondents (see Table 4).

Systematic sampling based on picking every n th person where $n = \frac{\text{population size}}{\text{sample size}}$ (1)

In all, there were 300 employees which were divided by ten, yielding a total of three. Every third individual was chosen here. As a result, the sample size was reduced to 30 persons. Each interviewee was issued an anonymous ID identification to maintain anonymity (Walsham, 2006), as indicated in Table 3.

Table 3. Employee Tags Used for Anonymity

Group of users	Number of users	Anonymous ID
Senior executive, CIO, CTO	3	IDR_SE_1, IDR_SE_2, IDR_SE_3
Marketing	3	IDR_MD_3
Junior Managers	6	IDR_JM_6
Financial Department	4	IDR_FD_4
IT-Staff	6	IDR_IT_6
DevOPs	8	IDR_DO_8

During the analysis phase, the interview data was classified to find any issues regarding factors hindering ISP development. These interviews were used to substantiate the framework codes in Figure 2 and to confirm the constructs used in this study. To determine the impact of our NFC model, the interviews were conducted before and after the NFC. Morgan & Krueger (1998) suggests that focus groups should be avoided due to their divergent nature leading to a more structured view in the

organisation. To overcome this problem, all employees were interviewed in both normal social interactions and form. The problems we derived during this phase are summarized in Table 4.

Table 4. Reasons for ISP violation

Issue	Source	NFC Construct	Mitigation Method
Lack of in-depth knowledge of the organisation's current information security situation.	IDR_SE_2, IDR_FD_4	Security Intelligence	Increase awareness of information security among employees.
Lack of cyber threat information shared among peers.	IDR_SE_2, IDR_DO_2	Cyber Threat Intelligence	Raise employee awareness of current cyber threats.
Influence of external partners on decision-making.	IDR_SE_1	External Partners	Define ways in which external stakeholders can positively influence information security awareness programs.
Lack of leaders participating in ISP projects.	IDR_SE_2	organisational Commitment	Improvement of the ISP perception of the leaders.
Misperception of information security among managers and employees.	IDR_SE_2, IDR_SE_3, IDR_MD_3, IDR_IT_4	Information Security Misperception	Personal persuasion meetings with senior members.
Lack of or insufficient budgets for information security programs.	IDR_JM_6	Information Security Investment	Increasing the budget for information security training programs

After this phase, the six constructs coded in Figure 2, as shown in Table 5, were confirmed to be the most important factors for ISP development and implementation.

	NFC Constructs	Definition
1	Security intelligence	A sound knowledge of the organisation's current security situation.
2	Cyber threat intelligence	The cyber threat information shared among peers.
3	External partners	External influence on ISP implementation.
4	organisational commitment	Managers participating in ISP projects have a positive impact on ISP development.
5	Information security misperception	Security misperception is based on security know-how and know-why.
6	Information Security Investment	IT security budgets are essential to ISP development.

As shown in Figure 3, the six coded key constructs and the central point are encapsulated in the control integration and close gaps dynamic of the NFC as in the work of Stewart & Jürjens (2017).

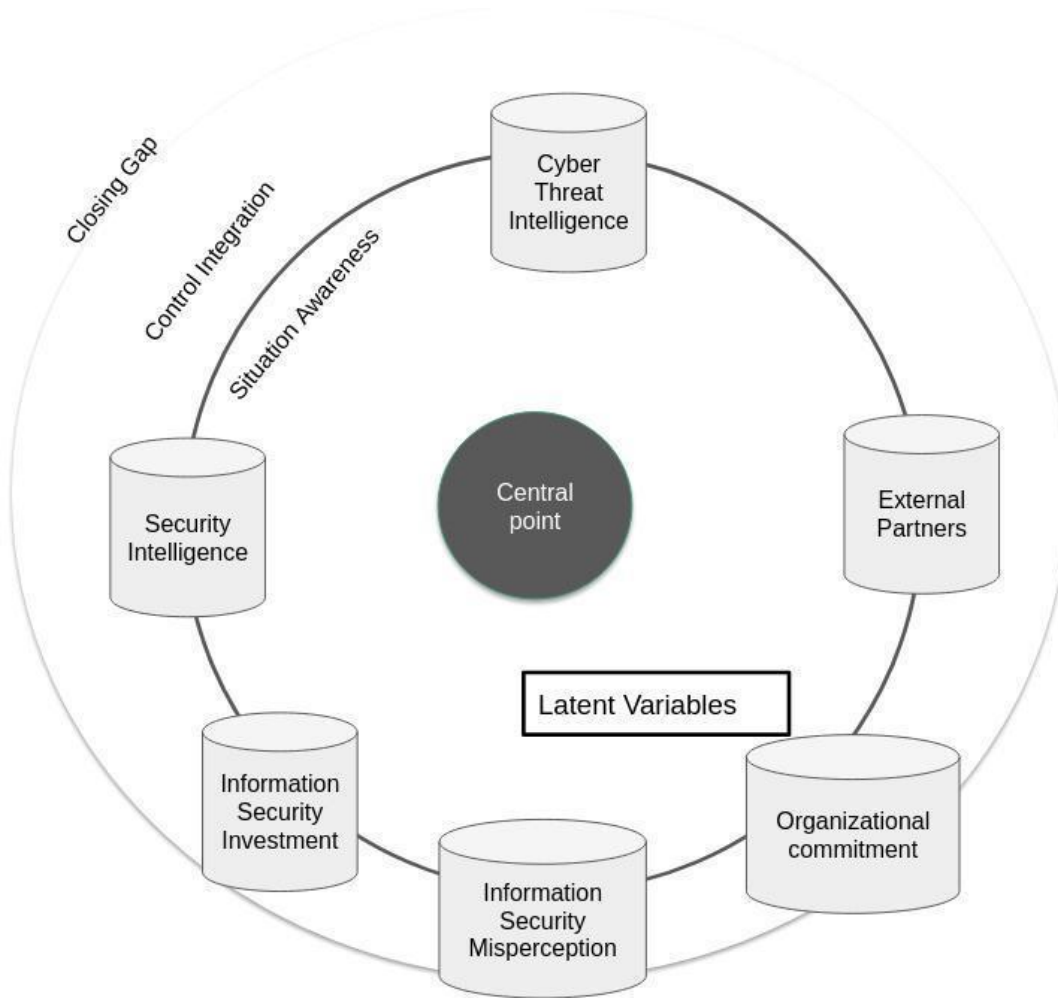


Figure 3. Framework for analysing the functioning of an ISP Development based on the NFC approach

The internal constructs that are retained at the "central point" are the six constructs of an ISP development in this paper, i.e. the structural constructs on which its foundation is based. The constructs have been defined based on the data analysis of the organisation. Besides the "central point" as shown in Figure 3 are other latent variables and elements considered as the choices that can be made based on the decisions of the organisation to implement the ISP.

At this stage, the six major constructs are involved in the dynamics of control integration and gap closure, as shown in Figure 3. Security intelligence, which includes (individual awareness of the ISP and its practices), is placed at 9 o'clock; cyber threat intelligence, which includes (the severity of an information security threat, knowledge, and expertise), is placed at 12 o'clock; external partners, which includes (external, regulatory, competitive, and social pressures), is placed at 3 o'clock; organisational commitment, which includes (motivation and perceived punishment for noncompliance with ISP or

reward), is placed at 5 o'clock; information security misperception, which includes (information security knowledge management, perception of self-efficacy to comply, and controllability), is placed at 6 o'clock; and investment in information security projects is placed at 7 o'clock. Although there was no certainty that their current positions would remain or change during the process. The constructs are shown in table 5.

4.3. Background and Participants

The proposed study is applied to describe the main features of a multinational organisation 's ISP implementation program and how it can contribute to explain success constructs and critical points.

The ISP system was implemented with the specific objective of shortening the project life cycle and improving the performance of the organisation. Due to the nature of the business, a better use of the experience and implicit knowledge of the employees was considered essential. Therefore, we designed the ISP system so that this experience could be used to prevent the repetition of mistakes or, more importantly, to realize the full potential of each employee. Communication and cooperation between humans was of great importance for the ISP system.

First the two "external elements" are defined. Both represent the overall constraints and opportunities in which the program has been designed, constructed and implemented (the business environment and the company's information security knowledge strategy). Then the six constructs that characterize the "internal" features of the ISP system are analyzed.

The company in this work is a multinational company with activities in the three main service and utility sectors traditionally managed by public authorities - water management, waste management and energy services, with more than 419,922 employees in 72 countries of different nationalities. It is the fastest growing innovative company in Germany in the last decade: current production is 2.1 million sales per day; in 2019 net profit was over 9.8 billion euros. The research was conducted with all the employees, and took place over a 12-month period from September 2018 to August 2019. The company's business is very complex and requires a great variety of activities and professional skills. Technical skills include several specializations (construction, geology, electronics, mechanics, chemistry, etc.). The organisation brings together experts from different disciplines and with mutual skills on an exceptionally global scale. Economic leadership skills are also vital, not to mention the judicial and political skills needed for international negotiations and contract signing. A consequent challenge is to integrate the different insular of information security knowledge specialisation around the department

and to ensure a balance between the efficiency required for routine activities and the innovation required in new projects. All this highlights a first important issue relevant to ISP development and implementation.

The entity has pursued a centralised ISP strategy for all units in all its branches, but the development and implementation of ISPs requires different skills and different steps of the project - from ISP strategy to implementation on site.

4.4. Problem Identification

As a rule of thumb, we conservatively rotated the NFC 8 times ($8 \times 5 = 40$) to identify the most important constructs to prioritize, as in the work of Stewart & Jürjens (2017). During this rotation phase, it became clear that the ISP strategy pursued by the organisation is mainly designed to establish an ISP strategy that facilitates the exchange of knowledge between all branches of the company by eliminating the spatial constraints due to the global spread of the employees. According to the organisation, this strategy reduces the cost of implementing different ISPs at different locations. Their current ISP was also focused on professionals of the organisation, operational departments and the more experienced employees, and neglected both the leaders and the entire staff members.

The leaders showed less commitment to ISP strategy. A resulting challenge was their misperception of what an ISP is. This misperception connects the various critical constructs, such as cyber threat intelligence, security intelligence, the budget for information security programs for the entire department, and ensuring a balance between the efficiency required for day-to-day operations and the innovation required in the development and implementation of an ISP.

The professionals were considered the key success factor of their strategy, and the ISP system was built around these humans and their behaviors. However, it was clear that the implementation of such a strategy would have required some kind of supporting structure to facilitate the development of the ISP system, help the professionals to carry out the practical activities and maintain a link with top management. Furthermore, the ISP program should have involved the line operators and staff members, without forcing them to make unjustified efforts. The IT leaders recognized the issues faced by the organisation and saw the need to improve current security measures to better manage and secure valuable assets. Table 6 shows a table of the issues recognized.

Table 6: Current ISP issues at the entity

	Overall ISP support in percentage (%)			
	2016	2017	2018	2019
ISP construction	35%	28%	19%	18%
ISP compliance and enforcement	5%	4%	15%	12%
Management support	13%	7.5%	1%	3.2%
Risk assessment	3%	2%	5%	10%
Employee support	5%	6%	2%	1%
Stakeholder support	1%	0.5%	3%	3.1%
ISP policy implementation	1%	1%	0.5%	0.1%
ISP monitoring	0%	0%	0%	0%
International security standards	26%	31%	20%	31%
Law and regulation requirements	40%	39%	31%	22.5%

To further analyse the six coded constructs and find out what should be tackled first in ISP development, the six constructs were iteratively sampled by the means at each iteration of 8 iterations. This enabled the re-order of the constructs as shown in Table 7. Prior to mapping and re-mapping, the six constructs were analysed in general terms by using keywords and phrases to find the repetitive latent variables found in each construct, grouping the constructs into hierarchical concepts, and categorising the constructs by identifying relationships.

Table 7: Constructs mapping to the NFC clock

NFC Constructs	Constructs initial positions	Constructs positions after 8 times repetition
External partners or Stakeholders	3 o'clock	9 o'clock
Information security misperception	6 o'clock	12 o'clock
Information Security Investment	7 o'clock	3 o'clock
Organisational commitment	5 o'clock	5 o'clock
Security Intelligence	9 o'clock	6 o'clock
Cyber Threat Intelligence	12 o'clock	7 o'clock

Finally, the categories formed in this way and the relationships found between the latent variables of the six constructs are used as the basis for repositioning the clock as shown in Figure 4.



Figure. 4 Constructs Prioritization

This approach allowed the researcher to reform the six constructs rather than simplistically placing them without rigid structure or prescribed rules. The absence of repositioning could lead to uncertainty about how to initiate the NFC process. This phase of problem analysis allowed the researcher to prioritize the constructs shown in Figure 4, which were used chronologically to develop this study. This is also listed in table 7.

5.0. Developing the Information Security Program

The 12-month research consisted of two research cycles. The first phase of the research began in the period from September 2018 to June 2019 and consisted of the implementation of the ISP. This implementation was based on the six constructs derived during the data analysis in Table 5 and mapped to the NFC framework in Figure 2. The second phase, also known as the evaluation phase, began in July 2019 and was completed in August 2019.

5.1. Phase One

The six constructs are discussed in more detail in this Phase.

(i) External Partners (Stakeholders & Regulators)

Stakeholders or external partners play a major role in this work. During the interview, the researcher was informed about the pressure stemmed from stakeholders to comply with certain information security rules. The organisation is forced to adopt certain institutionalized rules and practices in the development and management of the ISP (Hu et al., 2007). This pressure can hinder the progress of ISPs, as the organisation must adopt various information security practices that are not directly addressed to the organisation needs, but can provide the basis for establishing a resilient response to regulatory demands.

To solve this issue, the research team including the top managers met up with the stakeholders to clear any misperception. This meeting enabled the research team to develop a strategic ISP approach that benefits both the organisation and external partners. According to Khansa & Liginlal (2007), the strategic approach to developing a strategic ISP is to integrate regulatory requirements into its information security practices in order to meet legal obligations and obtain a strategic ISP that is aligned with its business.

(ii) Information Security Misperception

Information security misperceptions are based on several factors that prevent an organisation from developing a well-defined ISP. Several research studies have attempted to identify the various reasons for the varying degrees of challenges in ISP development. The academic literature and reports from information security institutions on ISP development have been examined, and the factors influencing this development have been classified into three categories: organisational, human and technological. In Kraemer et al. (2009), the authors emphasise that organisational and human factors are directly related to information security vulnerabilities, and Stewart (2020) also highlights how the relationship between humans and technology can improve information security. ISP development would be a difficult task without user interaction, so controlling user behaviour in relation to these policies is key to success.

Misperception of security leads to several vulnerabilities in the security chain, such as shadow IT (see Figure 4). Shadow IT hinders the adoption of ISPs (Stewart & Jürjens, 2017; Kirlappos et al., 2015). Shadow IT can be defined as the use of IT systems without adherence to the organisation's IT system usage policies. In addition, with the adoption of cloud computing, shadow IT can be redefined

as the misuse of the organisation's IT systems and the storage of critical information in an unapproved location.

These employees implement their own security solutions when they feel that the ISP exceeds their capacity or affects their productivity.

The relationship between humans and technology plays an important role. ISP development and implementation would be a difficult task without user interaction, so controlling user behavior in relation to ISP is key to success. Most misperceptions of information security are (i) perception (Huang et al., 2011), (ii) personality (Mcbride et al., 2012), (iii) technology democracy (Colwill, 2009), (iv) cultural constructs (Greene & D'Arcy, 2010), (v) gender (Hanley et al., 2011), (vi) satisfaction (Xue et al., 2011), and (vii) habits (Herath & Rao, 2009).

Despite the positive impact of technology on society, workers with limited computer skills are vulnerable to phishing attacks. Lack of information security can leave humans exposed to cyberattacks. Older humans in a company are more likely to be targeted by fraudsters. A recent survey found that humans over the age of 65 are 35% more likely to lose money to financial fraud than humans under the age of 30. Employees need to be educated about cyber threats and security awareness training should be offered regularly to dispel misconceptions about IS. Vroom & Von Solms (2004) suggest continuous training and communication.

After the perception improvement phase, employees as well as management and stakeholders were identified and they were more than willing to participate in this project.

(iii) Investment in ISP projects

The next step was to increase the budget for the project. This went smoothly as both the management team and the stakeholders were committed to the project and more than willing to ensure its success. This success can be attributed to the perception enhancement phase, which was the first step in the development process (see 4.5.1). Organisations should consider a cyber security risk assessment when planning their budget. This should weigh the cost to the organisation against the likelihood of a threat occurring. Decisions to purchase cyber security tools must be effectively analyzed to support the development of the ISP. Organisations must invest in security projects such as, providing security-awareness and training staff members on security matters. Here, both the cost of implementing a particular defence and the impact that defence has on the business must be addressed.

Most organisations' IT security budget is within the IT budget which forces the security management to implement defences that are within their limited budget.

Once the appropriate budget was established, the next step was to increase the commitment of all employees, executives, management, departments, and selected team leaders toward ISP development.

(iv) Organisational commitment (ISP project team identification)

At this stage, the construct of organisational commitment became a key construct in this work (Stewart & Jürjens, 2017; Leach 2003). The establishment of the ISP team by management demonstrates to employees the commitment of management. During the commitment phase, the board of directors identifies key stakeholders and defines roles and responsibilities. The involvement of relevant stakeholders throughout the organisation at all levels assigned in the ISP development process is a successful construct for the ISP development.

After the key stakeholders have been identified, the next phase was to define roles and responsibilities as part of the planning strategy. A clear definition of the roles and responsibilities of development team members is important to avoid delays in the development cycle due to human challenges and political interference (Whitman and Mattord 2010). Maynard et al. (2011) observes that while many researchers stress the importance of involving different stakeholders in the development process, the respective roles of these stakeholders remain vague. He also notes that the authors mention only the name of the stakeholder who needs to be involved in the development process, without clarifying what this group of humans is supposed to do in the event. Therefore, Maynard et al. (2011) and Stewart & Jürjens (2017) discuss the roles of individual stakeholders in the ISP development process. In this work, those given roles and responsibility are addressed as "Facilitators" as shown in Figure 5.

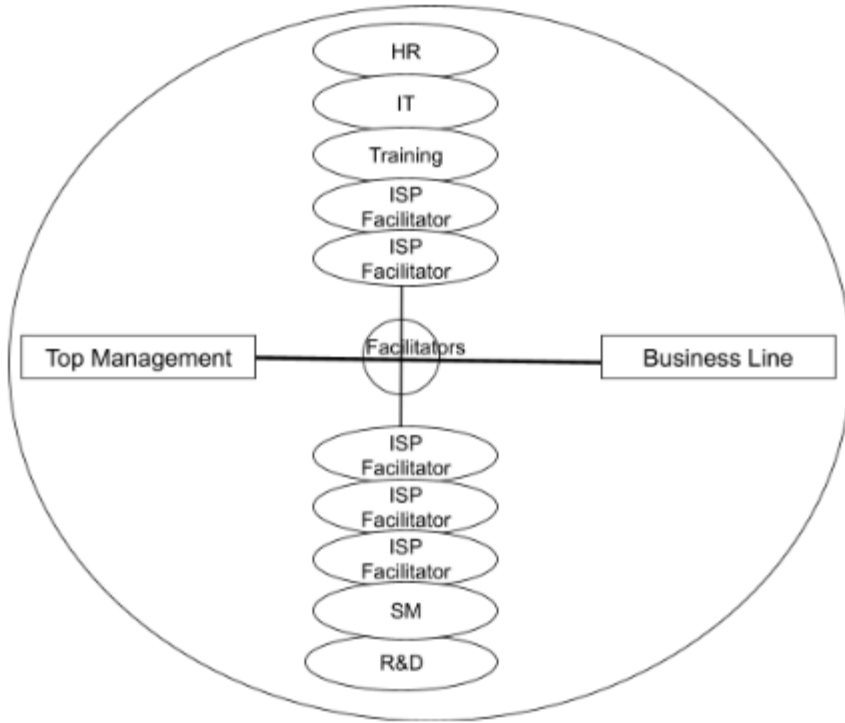


Figure 5. Empowerment Team: Composition and roles of facilitators

The work of the ISPs is supported by a special group, the so-called Empowerment Team, which consists of facilitators from the different divisions who share their experiences for the benefit of the entire ISP program, as well as representatives of other functions such as HR, IT, management, communication, etc., as shown in Figure 5. The main objective of the Empowerment Team was to promote the dissemination culture and good practices between the different departments. In this work, facilitators stand in the middle between top management and the business units. The Empowerment Team acts as a mediator between top management and all other departments. A Group Chief Information Security Officer (CISO), who leads the Empowerment Team, is specifically designated for this role. The Group CISO, the Empowerment Team and all departments are supported by the ISP Team, which consists of communication and ICT specialists.

The main idea for transparency in this project was to create a structured and systematic system to support each department. Although each department is free to make specific internal regulations, a common set of practices and rules was established. The approach currently pursued (Figure 4) can be seen as an attempt to achieve the difficult trade-off between efficiency and flexibility of the ISP system,

with the aim of ensuring participation on the one hand and avoiding conflicts with the formal structure and "daily" routines on the other.

After stakeholders and facilitators had been defined, the next step was to raise awareness of information security among employees and improve the perception of ISP.

The first step was to identify those involved in decision making and assign roles and responsibilities. These roles and responsibilities also included an ISP development unit, an audit unit, and an external tester unit. The roles and responsibilities are then implemented into the NFC model as in the work of (Stewart & Jürjens, 2017) as shown in Figure 6.

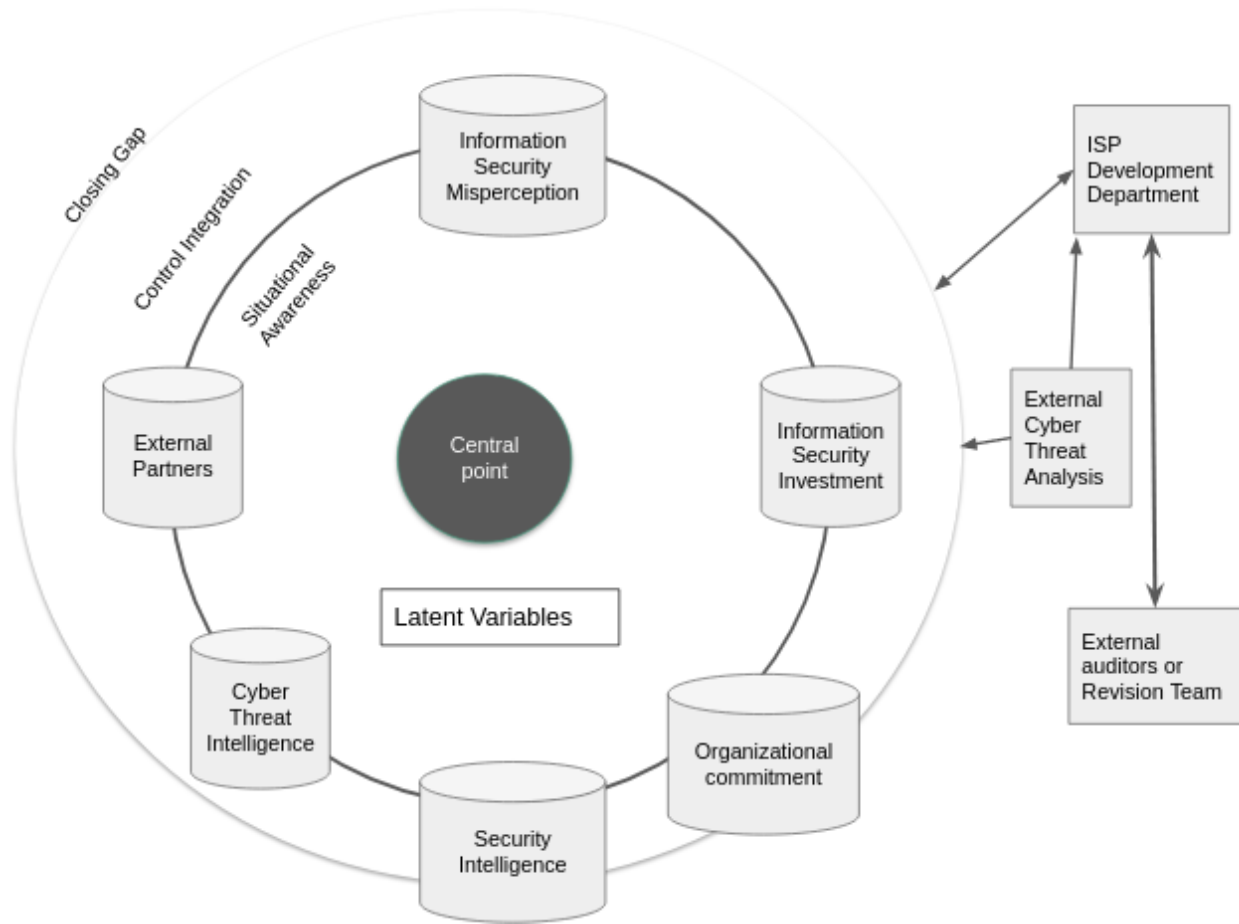


Figure 6. ISP system Development

(v) Security Intelligence

Security intelligence is essential for the development of a successful ISP. Once the strategy development team is in place, the organisation should identify its security needs (Whitman and

Mattord 2010). A sound knowledge of the organisation's current situation and a sufficient understanding of the organisation's security objectives are required (Ølnes 1994; Palmer et al. 2001; Stahl et al. 2012). This can be achieved by a detailed analysis of the organisation's problem (Whitman 2008). The identification of the organisation's security requirements consists of two activities: (a) Identification of the security needs and (b) Assessment of the organisation's current policies and procedures.

a. Identification of the security needs

The fact that organisations have different security requirements and objectives means that organisations have different security needs (Karyda et al. 2005; Ølnes 1994; Wood 2004). Baskerville and Siponen (2002) point out that when developing security policies it is essential to understand the security requirements of the organisation. Therefore, the organisation should identify its security objectives, including the level of security that the organisation intends to achieve. The security requirements should detail the organisation's needs to address security risks identified through a risk assessment in order to meet its security needs and achieve its business objectives. The result of the risk assessment is a contribution to the definition of security requirements, and should be considered during the initial phase of ISP development lifecycle (Stewart & Jürjens, 2017), but not for policy development (Rees et al., 2003).

b. Assessment of the organisation's current policies and procedures

The previous evaluation of the organisation's ISP and existing procedures had several advantages. In the first place, it enabled the ISP design team to gain an understanding of the state of the art of existing policies and practices (Doherty & Fulford 2006; Palmer et al., 2001; Rees et al., 2003; Whitman 2008). Secondly, it also enabled the organisation to identify gaps in the current policy and determine whether the existing policy helped the organisation manage risk by meeting its security requirements, thereby identifying areas that the new policy must address. Thirdly, the evaluation of existing policies and procedures ensured that the new policy met existing policy standards (SANS Institute 2001). This raised the probability of successful implementation of the revised policies throughout the organisation (Peltier, 2013). Lastly, the evaluation process helped to collect key materials such as existing policy and procedure documents that served as an important reference for the development team (Patrick 2002; Whitman et al. 2001). Inadequate organisational security intelligence may result in a deficiency of skills, know-how and capabilities in handling security demands (Greitzer et al., 2014). A study conducted by Siponen et al. (2014) found that information quality has a significant impact on

actual compliance with ISPs. In addition, Bulgurcu et al. (2010) investigated the influence of the three quality dimensions of clarity, adaptability and consistency on the compliance of employees with security rules and regulations and emphasized their importance.

(vi) Cyber Threat Intelligence

Threat Intelligence has been neglected in the development of ISPs. According to Stewart (2020), threat intelligence should be considered an important construct in the development of ISPs. The inclusion of Threat Intelligence topics in the ISP can help employees detect phishing emails and malware attachments. When employees know what a compromised site looks like, they become aware and can identify at the point where the hacker makes the request (either through phishing emails, vishing, or another source). Improving threat intelligence can alert employees to malicious attempts. These alerts can also enable them to take the right action, report incidents to the security department, which can then block traffic or quarantine the system. Thomson et al. (2006) propose the information security shared tacit espoused values (MISSTEV) model to enhance the cultivation of an information security culture.

The value of threat intelligence derived from within an organisation sits between the direct usefulness of specific knowledge about threats to the organisation (Padayachee, 2012). Threat information must be distributed to all employees and documented. This exchange of threat information can be a benefit to enhance the organisation's security defenses. Herath and Rao (2009) identify four key factors that influence ISP, namely threat perceptions about the severity of breaches, organisational commitment, social influences, and resource availability. Siponen et al. (2014) argue that employees' understanding of threat, vulnerability, and their severity, have a positive and significant impact on their intention to comply with ISPs. A strategic threat intelligence system was then set up to direct all departments of the organisation.

According to Stewart (2020), there is a shortage of security analysts and existing security teams are under constant pressure to deliver more with less. In the 2021 NFC model studied by Stewart, data security and consumer trust were critical during the study (Stewart, 2021; Stewart & Jürjens, 2018).

As a result, there is a constant need to train employees to improve their cyber security skills and ensure that all employees are involved in cyber defence. In short, security is everyone's responsibility. At this point, all employees were eager to learn more. They recognized the need for information security and

its benefits. All employees were given IS training. IT staff and the DevOPs team were trained in IT security best practices by an external organisation.

5.2. Evaluation of the Field Notes and Writing up of the Results

The method of this observation is based on a systematic approach. In doing so, the researcher focused on different types of activities to highlight the distinctions in this study (Angrosino & dePerez, 2000). Due to the considerable amount of time involved, the researcher had the opportunity to observe and participate in a variety of activities over time. Through these activities, the researcher was able to engage with the 30 members of the Company who were able to outline what the study meant to them as individuals and how they could use the findings to improve their current ISP development process. Trust was an essential component in building relationships to get participants to open up. Other best practices, including ethics, were considered to minimise researcher bias and maximise the efficiency of the field experience.

Since the study aims to test the proposed guidelines for understanding the six constructs for the success or failure of ISPs, a fundamental question must first be answered: *How and when is it possible to confirm that an ISP program is a success or failure?*

To find the answer to the question, the evaluation process was done systematically as in the work of Bishop et al. (1998). All participants were interviewed on two occasions. This took the form of both a personal interview and a group interview. In addition, participant observation was used to obtain further information. Overall, the results were positive. The CIO was positive about the awareness raising program.

“Two important elements can be mentioned in particular. During the first four months of implementation, we have estimated the value generated by the NFC framework in terms of cost savings and other economic indicators. These results are sufficient to cover approximately 31 times the total cost of our former ISP projects.”

The CTO saw the improvement of employees behavior and attitudes towards the ISP.

“The level of knowledge in the field of information security has grown over time, which can be seen as a change in the attitude and behavior of employees towards security awareness, which is also a key construct for the strategic goals of the company.”

Eleven employees also shared how the awareness program made them reflect on the implications of a data breach. According to these users, this increased their commitment to reading the ISP thoroughly.

“All indicators observed by the organisation seem promising. The interaction among employees on cyber security topics has increased, and we can now see an average of 21.2 interactions (e-mail exchanges as part of security awareness) per working day in 29 business domains, with a new element of security knowledge being produced every day.”

Furthermore, the senior executive who was interviewed in the beginning realized how the analysis of critical success constructs conducted with the help of the framework has helped to determine the reasons for these good results and pinpoint the constructs that can be regarded as shortcomings.

“The proposed framework has been able to enable the organisation to define a strategic ISP strategy that is strictly aligned with the business strategy as compared to our complex strategy. The proposed framework has enabled us to achieve a more effective and efficient use of the knowledge and skills of the more qualified and experienced employees.”

In summary, the constructs underlying the results obtained by the organisation can be identified and understood within the proposed framework and can be summarized by the following constructs:

- a well defined and focused ISP strategy;
- a strict alignment between the ISP strategy and the entire organisation;
- a balanced focus on all the different dimensions of ISPs; and
- a thorough consideration of the business and organisational context.

Table 8. Summary of the Results Achieved During the first phase

Issue	Method	Source of Evidence
Improved the costs associated with ISP programs.	Interview	IDR_SE_2
Improved the level of knowledge in the area of information security.	Interview	IDR_SE_3
Improved awareness and eliminated any misperceptions.	Interview	IDR_FD_2, IDR_DO_2, IDR_SE_1, IDR_MD_3, IDR_IT_4, IDR_JM_1, IDR_SD_1

Improved ISP strategy aligned with the organisation.	Interview	Senior Executive
Observed staff's understanding and commitment to ISP to dispel misconceptions.	Participatory observation	Researchers
Improved management willingness to invest in IS projects.	Participatory observation	Researchers
Observe the behavior of stakeholders and employees.	Direct Observation	External Auditors

In spite of the positive results summarized in Table 8, there were still additional issues to be addressed, as this research also provides an opportunity to identify specific weaknesses that the company may be able to work on.

1. The issue of measuring ISP-compliant activities is a controversial and problematic issue that still needs to be addressed. This is essential for the long-term sustainability of the ISP project and for the implementation of the budgeting process, which is also crucial for a full acknowledgement of the role of the ISP in the organisation.
2. In addition, the ISP program should continue to include the entire organisational line. In terms of ICT design, the system was kept simple: From the organisation's point of view, ISP success is about humans adhering to established policies, not about computing power.
3. As previously stated, the simplicity and ease of use of the framework is an essential construct that can contribute to the evolution of the ISP program throughout the organisation and for other organisations alike. However, it is likely that specific and more complex technologies might become indispensable.

To solve the three issues above, the first and second were addressed by continuing enhancing ISP strategies, communication, training and monitoring user activity based on ISP development, while the third was addressed by repeating the process whenever there was a change that impacted the current established ISP strategy.

6.0. ISP Success Factors

To achieve successful ISP development and implementation, six constructs for effective policy were considered, namely: (i) external partners or stakeholders, (ii) information security misperceptions, (iii) information security investment, (iv) organisational commitment, (v) security intelligence, and (vi) cyber threat intelligence.

This study found that an effective ISP is made up of various components, the most essential of which is that an ISP must be acceptable and usable by all employees including external partners and stakeholders. Thus the support of these individuals are essential for the success of ISP development. As a consequence, a high level of management engagement in ISP development, such as dedicating enough resources for the risk assessment process, would elevate the chance of success in the ISP design process.

The ISP is useless if an organisation or its workers are unable to apply the policies or regulations mentioned in the policy. As a result, removing misperceptions about information security and increasing employees' perceptions of the relevance of information security is a key success element in the development and implementation of ISPs.

Investing in employee ISP awareness and training also helps to preserve the security of sensitive data while reducing human mistake and negligence. Despite employees' willingness to embrace any changes, a continuous training endeavor is required rather than a one-time training session, which is a big investment for any organisation. Investing in ISP ensures continuing compliance, and with reputation and financial security at stake, the financial benefits of information security far outweigh the costs.

Organisational commitment contributes positively to the success of ISPs development and implementation, leading towards data security improvement. While the misconduct of an individual employee can have profound consequences for a company, the misconduct of top management can have catastrophic consequences. It is therefore crucial to convince leaders to fully embrace the information security measures that have been put in place, which means not only inspiring them to adhere to the security principles, but also to take on the obligations that come with the top positions.

Security Intelligence strives to promote the development of the ISP as it elevates the perceived significance of information security for employees, thus helping to build a security culture, an approach

that takes into account the best interests of all stakeholders and the characteristics of information systems (IS) and information technology (IT). Developing a culture of security requires both leadership and extensive collaboration, both of which promote ISP success. Designing and managing cybersecurity should be a key component of corporate governance, and all stakeholders must recognise the importance of security. Security culture should be the responsibility of each individual to help embrace and promote security culture as a way of thinking about the assessment and implementation of information systems and networks.

Humans play an important role in the security chain and their cyber threat intelligence contributes to the success of the ISP development and implementation. With the rise of everything from phishing emails to vishing, it is important that employees who access corporate computer systems and networks receive in-depth training on how to detect, report, ascertain, escalate and mitigate cyber threats. This can be achieved by describing in the ISP document how to behave in each situation and by training and testing employees. Due diligence must be conducted on external partners and suppliers to ensure they have appropriate cybersecurity protections in place to prevent attacks on the organisation information system. In short, a successful ISP requires all six constructs in this paper.

7.0. Discussion

The ISP developed for the organisation in this study was concise, clear and as comprehensive as possible to provide the information needed to implement the rule. It was given a version number and a date so that the most current version could be quickly identified, and it was internally organized such that relevant or necessary information could be quickly identified and located within the document. Other factors, such as the usage of established or implied regulations, were also taken into account (Flowerday & Tuyikeze, 2016; Tuyikeze & Flowerday, 2014; Lucila, 2016; Stewart, 2020).

The ISP designed in this work aimed to improve the confidentiality of ongoing processes and not to hinder or disrupt business operations (Stewart & Jürjens, 2017; 2018). Where necessary, appropriate technical means were used to enforce the policy, and where this was not possible, sanctions were imposed. As not all formulated policies could be enforced through automation, manual processes were specified in the policy document (Stewart, 2020).

Local and national laws were taken into account as the organisation in this study follows many ordinances and laws that regulate the protection of certain records, dealing with outsiders and

violation of access. Therefore, the policy was endorsed by the legal department, which is familiar with the laws in its industry and environment (Wiander, 2009).

Other topics covered in the ISP policy include: an acceptable use policy, an anti-malware policy to protect computer systems, an email policy that covers the use of company email accounts and addresses, a clean desk policy, an internet security policy that covers internet usage, a password policy that ensures strong passwords, a removable media policy, and a security response plan policy that covers the use of company email accounts and addresses.

Being aware that a useless and non-compliant policy is useless, an audit procedure has been put in place to verify compliance and to determine the punitive measures that can be taken in case of non-compliance with any of the prescribed provisions. The interests of employees, customers, partners and the company's business objectives were considered in the ISP document.

Before the ISP document was finalised, a draft was sent to various departments for review. In this way, a representative document was created that addressed the concerns of all interests within the company. The document also included purchasing decisions, persons to be notified in certain situations, detailed remedial actions to be taken after a breach, and any legal or criminal sanctions. Other areas addressed in the document were data protection, legal issues, human resources and management.

As the ISP is an ongoing process and not a product, the organisation was advised to regularly and periodically review and update the ISP document to ensure that it is up to date and covers all applicable situations, environments and systems within the organisation (Lucila, 2016; Stewart & Jürjens, 2017).

Other features considered was the purpose of the policy, to uphold the organisation's reputation and fulfil its ethical and legal obligations. Next, the humans within and outside the scope to whom the ISP applies were considered. With management approval, the policy was clearly defined and its objectives focused on the confidentiality, integrity and availability of its critical assets. To ensure that data could be shared and with whom, both authority and access control policies were considered. The data was categorised as public, private and confidential. Other features considered in this work were data protection regulations such as industry standards, organisational standards, relevant regulations and best practices in handling personal data. To ensure that the policy is conveyed to the target audience, security awareness training that covers data protection measures is provided. These security awareness

training improve the knowledge of trainees about cyber threats and highlight their responsibility to detect, avoid and report such incidents (Stewart & Jürjens, 2017; Vroom & Von Solms, 2004).

8.0. Implications

This study uses the NFC framework to explain influences on ISP development and outcomes (e.g., company X). The study took place in a multinational, complex organisation with diverse staff, cultural backgrounds, and perspectives. Based on this work and the data collection, it has been propose that the six construct that can influence ISP development and outcomes can be grouped into six categories: external partners or stakeholders, (ii) information security misperceptions, (iii) information security investment, (iv) organisational commitment, (v) security intelligence, and (vi) cyber threat intelligence.

This study has significant implications for practice. First of all this is the first academic study to investigate ISP development in organisations based on the NFC framework. In addition, it is the first study to use the NFC framework to explicate influences on ISP development and outcomes in information security research. The framework provides a new perspective to examine organisational ISP development strategy and some success factors. This work has justified the applicability of the NFC framework to explain the actions required in ISP projects by systematically testing the interrelationship among all six constructs which also answers the research question.

This study has presented a new perspective to explain why ISP development and implementation is not a one-man responsibility, but various factors that must work together to develop an ISP. In practice, this study can serve as a reference for managers to set up a strategic ISP highlighting the context of IS to improve staff perceptions, e.g. through training to better inform staff.

Although latent variables such as awareness raising and training play an important role in staff behaviour, they are not the main key to developing a strategic ISP. Therefore, strategic ISP can be achieved by combining the six constructs in this study by arranging them in a structured manner towards effective ISP development and implementation.

Consequently, a high level of management commitment to ISP development, such as allocating sufficient resources to the risk assessment process, would increase the chances of success in ISP design.

In addition, the significant relationship between employee support and the six constructs may impact the expected outcome of ISP. Therefore, a high level of ISP support from employees can increase the possibility of a successful ISP implementation.

9.0. Limitations

First, the study took place in Germany and most of the data was collected virtually due to the different locations of the organisation. As this is the first attempt to test the framework in a large enterprise, further empirical research is needed. In particular, it would be particularly useful to apply the framework to cases of failure. Therefore, this study cannot be generalized to all organisations, and thus future research is needed to examine other business environments.

10.0. Conclusion

The research question raised in this thesis is what procedures organisations should follow to develop and implement an effective information policy. The list of six constructs that emerged from this work has been analysed and interpreted so that a model for the development of an ISP could be derived.

The outcomes of our proposed framework shows its usefulness as a tool for analysing the vital elements of an ISP development program. The framework seems suitable for a solid and structured analysis of the functioning of current ISPs and for figuring out the reasons behind their success or failure. Consequently, it may also be useful to test the framework in cases of failure. In spite of this, the availability of a systematic approach, as the one proposed here, appears to be an important contribution to the development of this field.

It is obvious that further empirical studies are needed to validate or adapt the framework more effectively. It would be particularly useful to extend it to other situations in the same industry comparisons and cross-analyses. Alternatively, it could be applied to other sectors which may emphasise completely different elements. Furthermore, it could be useful to test the framework for cases of failure.

Nevertheless, the existence of a systematic framework such as the one proposed here appears to be an essential contribution to the development of this sector.

This study emphasizes the value of awareness-raising initiatives in relation to ISP and serves as a motivation to give priority to an appropriate ISP and its communication to employees. This will serve as motivation to bridge the gap between the proportion of organisations that have no initiatives to raise awareness of their ISP and the percentage of organisations that have such initiatives.

This paper also provides a comprehensive guide for practitioners on the activities that security managers need to undertake in developing security policies, and allows practitioners to compare their current practice with the proposed models for good practice. The main contribution of the paper is the application of a comprehensive and coherent model that can be the first step in defining a "checklist" for creating and managing ISPs. The suggested model encompasses all dimensions that a company should take into account when developing and implementing ISPs. It ensures comprehensive and sustainable ISP strategies.

References

- Alhanahnah, M.J., Jhumka, A. and Alouneh, S. (2016). A Multidimension Taxonomy of Insider Threats in Cloud Computing. *The Computer Journal*, 59(11), pp.1612–1622.
- Baskerville, R., Siponen, M. (2002), "An information security meta-policy for emergent organisations", *Logist. Inf. Manage.* 15 (5/6), 337–346.
- Bishop, Doak & Reed, L. (1998) "Practical Guidelines for Interviewing, Selecting and Challenging Party" Appointed Arbitrators in International Commercial Arbitration, *Arbitration International*.
- Bjorck, F. (2004), "Institutional theory: A new perspective for research into IS / IT security in organisations," in *Proceedings of the 37th Hawaii International Conference on Systems Sciences*, 2004, vol. 0, no. C, pp. 1–5
- Britten N. (1999), "Qualitative interviews in healthcare", In Pope C, Mays N (eds) *Qualitative research in health care*. 2nd ed. pp 11–19. London: BMJ Books.
- Britten, N. (1995), "Qualitative Interviews in Medical Research", *BMJ (Clinical research ed.)*. 311. 251-3. 10.1136/bmj.311.6999.251.
- Bulgurcu, B., Cavusoglu, H., Benbasat, I.(2010), "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly*, vol. 34, no. 3, pp. 523-548.

- Colwill, C. (2009), "Human constructs in information security: The insider threat – Who can you trust these days?," in *Information Security Technical Report*, 2009, vol. 14, no. 4, pp. 186–196.
- CyberSecurity Insider (2014), "Insider threat Report", Available:
<https://www.cybersecurity-insiders.com/wp-content/uploads/2019/11/2020-Insider-Threat-Report-Gurucul.pdf>
- D'Arcy, J., Hovav, A., & Galletta, D. (2009), "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Inf. Syst. Res.*, vol. 20, no. 1, pp. 79–98, Mar. 2009.
- Doherty, N. F., Anastasakis, L., & Fulford, H. (2011), "Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy," *Int. J. Inf. Manage.*, vol. 31, no. 3, pp. 201–209, 2011.
- Doherty, N.F., and Fulford, H. (2006), "Aligning the Information Security Policy with the Strategic Information Systems Plan," *Computers & Security* (25:1), September , pp 55-63.
- Eloff, J.H.P & Eloff M.M. (2005), "Information security architecture", *Computer Fraud & Security*, Volume 2005, Issue 11, 2005, Pages 10-16, ISSN 1361-3723,
[https://doi.org/10.1016/S1361-3723\(05\)70275-X](https://doi.org/10.1016/S1361-3723(05)70275-X).
- Flowerday, S. V., Tuyikeze, T. (2016), "Information security policy development and implementation: The what, how and who," *Comput. Secur.*, vol. 61, pp. 169–183.
- Forrester (2021), "Cybersecurity prediction 2021" , Available:
<https://www.code42.com/resources/reports/forrester-paper-predictions-2021-cybersecurity>
- Gelles, M.G., (2016), "Insider threat: Prevention, detection, mitigation, and deterrence".
Butterworth-Heinemann. 17
- Goel, S., & Chengalur, I. N. (2010), "Metrics for characterizing the form of security policies," *J. Strateg. Inf. Syst.*, vol. 19, no. 4, pp. 281–295.
- Greene, G. and D'Arcy, J. (2010), "Assessing the Impact of Security Culture and the Employee-organisation Relationship on IS Security Compliance," in *5th Annual Symposium on Information Assurance*, 2010, pp. 1–8.

- Greitzer, F.L., Strozer, J., Cohen, S., Bergey, J., Cowley, J., Moore, A., and Mundie, D. (2014), "Unintentional Insider Threat: Contributing constructs, Observables, and Mitigation Strategies," in 2014 47th Hawaii International Conference on System Sciences, pp. 2025–2034.
- Hallsworth, R. M., and Parker, S. (2015), "Policy Making in The Real World: Evidence and Analysis,".
- Hanley, M., Dean, T., Schroeder, W and Houy, R. (2011), "An Analysis of Technical Observations in Insider Theft of Intellectual Property Cases," 2011.
- Herath, T and Rao, H.R (2009), "Protection Motivation and Deterrence: a Framework for Security Policy Compliance in organisations," *Eur. J. Inf. Syst.*, vol. 18, no. 2, pp. 106–125.
- Ifinedo, P. (2014), "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition," *Inf. Manag.*, vol. 51, no. 1, pp. 69–79, Jan. 2014.
- ISO/IEC 27002. Code of practice for information security management.
- Ishikawa, K. (1985) *What Is Total Quality Control The Japanese Way*. Translated by Lu, D.J., Prentice-Hall, Englewood Cliffs, New Jersey.
- Karyda, M. Kiountouzis, E., and Kokolakis, S. (2005), "Information Systems Security Policies: A Contextual Perspective," *Computers & Security* (24:3), pp 246-260.
- Khansa, L., & Liginlal, D. (2007), "The Influence of Regulations on Innovation in Information Security", *Proceedings of the American Conference on Information Systems*. pp. 18.
- Knapp, K. J., Franklin, M. R., Marshall, T. E., Byrd, T.A. (2009), "Information security policy: An organisational-level process model," *Comput. Secur.*, vol. 28, no. 7, pp. 493–508.
- Kirlappos, I., Parkin, S and Sasse, M.A. (2015), "Shadow Security' as a tool for the learning organisation," 2015, vol. 45, no. 1, pp. 29–37.
- Kraemer, S., Carayon, P and Clem, J. (2009), "Human and organisational constructs in computer and information security: Pathways to vulnerabilities," *Comput. Secur.*, vol. 28, no. 7, pp. 509–520.
- Kusserow, R. P. (2014), "Developing and Managing Compliance Policy Documents," *J. Heal. Care Compliance*, no. June, pp. 27–31.
- Leach, J. (2003), "Improving user security behavior", *Computers & Security*, Vol. 22, No. 8, pp 685–92.
- Lucila, N. B. (2016) , "Information Security Policy Development: A Literature Review," *Int. J. Innov. Res. Inf. Secur.*, vol. 3, no. 4, pp. 1–7

- Mattord, H.J., Levy, Y. and Furnell, S. (2014), "Factors for Measuring Password-Based Authentication Practices", *Journal of Information Privacy and Security*, 10(2), pp.71–94.
- Mauritian, C. T. (2011), "Guideline on Information Security Policy," Mauritius.
- Maynard, S., & Ruighaver, A. (2006), "What makes a good information security policy: a preliminary framework for evaluating security policy quality," in *Proceedings of the fifth annual security ...*, 2006, pp. 1–15.
- Maynard, S., Ruighaver, A., and Ahmad, A. (2011), "Stakeholders in Security Policy Development," 9th Australian Information Security Management Conference, December , pp 182-188.
- Mcbride, M., Carter, L. and Warkentin, M. (2012), "Exploring the Role of Individual Employee Characteristics and Personality on Employee Compliance with Cybersecurity Policies 1," 2012.
- Morgan, D. L., & Krueger, R. A. (1998). *The focus group kit*. Thousand Oaks, CA: Sage. Google Scholar.
- Myers, M., and Newman, M. (2007), "The Qualitative Interview in IS Research: Examining the Craft," *Information and organisation* (171), pp. 2-26.
- Neuman, W. L. (2007), "Basics of social research": Qualitative and quantitative approaches(2nd ed.). Boston, MA: Allyn and Bacon.
- Ølnes, J. (1994), "Development of Security Policies," *Computers & Security* (13:8), pp 628-636.
- Padayachee, K. (2012), "Taxonomy of compliant information security behavior", *Computers & Security*, Vol 31, No. 2012, pp673-680.
- Palmer, M.E., Robinson, C., Patilla, J.C., and Moser, E.P. (2001), "Information Security Policy Framework Best Practices for Security Policy in the E-Commerce Age," *Information Systems Security* (10:2), May , pp 1-15.
- Patrick, D.H. (2002), "The Security Policy Life Cycle," in: *Information Security Management Handbook*, Fourth Edition, Volume 4. Auerbach Publications, pp 297-311.
- Rees, J., Bandyopadhyay, S., and Spafford, E.H. (2003), "PFIRS: A Policy Framework for Information Security," *Communications of the ACM* (46:7), pp 101-106.
- SANS Institute. (2001), "Security Policy Roadmap - Process for Creating Security Policies."

- Sax, L. J., Gilmartin S. K. and Bryant A. N. (2003), "Assessing response rates and non response bias in web and paper surveys," *Research in Higher Education*, 44, 4, 409-431.
- Singh Lodhi, M. and Kaul, R. (2016). Detecting Unknown Insider Threat Scenarios. *International Journal on Computational Science & Applications*, 6(5/6), pp.15–21.
- Siponen, M., & Willison, R. (2009), "Information security management standards: Problems and solutions," *Inf. Manag.*, vol. 46, no. 5, pp. 267–270, Jun. 2009.
- Siponen, M., Mahmood, A. and Pahnla, S. (2014), "Employees' adherence to information security policies: an exploratory field study", *Information & Management*, Vol. 51, No. 201, pp217–224.
- Stahl, B.C., Doherty, N.F., and Shaw, M. (2012), "Information Security Policies in the Uk Healthcare Sector: A Critical Evaluation," *Information Systems Journal* (22:1), pp 77-94.
- Stewart, H., and Jürjens, J. (2017), "Information security management and the human aspect in organisations", *Information & Computer Security*, vol. 25, no. 5, pp. 494–534.
<https://doi.org/10.1108/ICS-07-2016-0054>.
- Stewart, H. and Jürjens, J. (2018), "Data security and consumer trust in FinTech innovation in Germany", *Information and Computer Security*, Vol. 26 No. 1, pp. 109-128.
<https://doi.org/10.1108/ICS-06-2017-0039>.
- Stewart, H. (2020), "Information Technology and Cyber Security Unplugged": The interrelationship between Human Technology and Cyber Crime Today (English Edition), Rohhat LTD" 2020.
- Stewart, H. (2021), "The hindrance of cloud computing acceptance within the financial sectors in Germany", *Information and Computer Security*, Vol. ahead-of-print No. ahead-of-print.
<https://doi.org/10.1108/ICS-01-2021-0002>.
- Soomro, Z. A., Shah, M. H., and Ahmed, J. (2016), "Information security management needs more holistic approach: A literature review," *Int. J. Inf. Manage.*, vol. 36, pp. 215–225.
- Sohrabi, N., Von Solms, R., Furnell, S., Elizabeth, P., and Africa, S. (2016), "Information security policy compliance model in organisations," *Comput. Secur.*, vol. 56, pp. 1–13.
- Thomson, K., Van Solms, R. and Louw, L. (2006), "Cultivating an organisational information security culture", *Computer Fraud and Security*, Vol. October, pp7-11.

- Tuyikeze, T., Flowerday, S. (2014), "Information Security Policy Development and Implementation: A Content Analysis Approach," in Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance, 2014, no. Haisa, pp. 11–20.
- Umbach, P. D. (2004), "Web surveys: Best practices," *New Directions in Institutional Research*, 121, 23-38. Bosnjak, M. Tuten T. L. and Bandilla W. (1991) Participation in web surveys: a typology, *ZUMA Nachrichten*, 48, pp. 7-17.
- Vroom, C. & Von Solms, R. (2004), "Towards information security behavioural compliance", *Computers & Security*, 23(3), 191-198.
- Waddell, S. A. (2013) "A Study of the Effect of Implementing Information Security Policy on Information Security Culture and Information Security Effectiveness in an organisation,".
- Walsham, G. (2006), "Doing Interpretive Research," *European Journal of Information Systems* (15:3), pp. 320-330.
- Whitman, M.E. (2008), "Security Policy: From Design to Maintenance," in: *Information Security : Policy, Processes, and Practices. Advances in Management Information Systems*.
- Whitman, M.E., Townsend, A.M., and Aalberts, R.J. (2001), "Information Systems Security and the Need for Policy,").
- Whitman, Michael & Mattord, Herb. (2015). *Principles of Information Security*, 5th Edition.
- Wiander, T. (2008), "Implementing the ISO/IEC 17799 standard in practice-experiences on audit phases," *Conf. Res. Pract. Inf. Technol. Ser.*, vol. 81, no. Aisc, pp. 115–119.
- Witmer, D. F. Colman, R. and Katzman, S. L.(1999), "From paper-and-pencil to screen-and-keyboard: Towards a methodology for survey research on the Internet, in Jones, S. (Ed.) *Doing Internet Research: Critical Issues and Methods for Examining the Net*. London. Sage. pp. 145-161.
- Wood, C.C. (2004), "Information Security Policies Made Easy : A Comprehensive Set of Information Security Policies", Houston : InformationShield, c2005. Version 10.0.
- Xue, Y., Liang, H. and Wu, L. (2011), "Punishment, justice, and compliance in mandatory IT settings," in *Information Systems Research*, 2011, vol. 22, pp. 400–414.

Chapter 10. Conclusion

The final chapter summarises the thesis. Stemming from the six research papers that were the subject of this thesis, this chapter provides an overall conclusion to this body of research and theoretical and managerial implications. In addition, limitations are explored, and suggestions for future research are made.

10.1. Overview

Over the years, the significance of cybersecurity in IS and DT has grown tremendously. However, studies have yet to be conducted to address the significant security challenges associated with these innovations. Existing literature on IS and DT mainly focuses on their strategies, innovation, and value creation (Tashtoush, 2021; Stewart & Jürjens, 2018; Agyaben et al., 2019; Aydiner et al., 2019), while neglecting the crucial security perspective (Agyaben et al., 2019; Aydiner et al., 2019). Therefore, it is imperative to develop a cybersecurity model that enhances IS and DT from a security perspective (Medlin, 2006).

This research has provided insights into managing cybersecurity challenges in DT and their corresponding control measures. The literature on IS and DT was carefully reviewed in Chapters 4, 5, 6, and 7 to identify significant constructs supporting the proposed NFC model (Stewart, 2022; Medlin, 2006; Cooper & Schindler, 2006; Ghauri & Gronhaug, 2005; Yin, 2014, p. 19; Umbach, 2004). Qualitative research was then conducted to determine the relevance of these constructs, while the quantitative research design and pilot study were discussed in detail. (Cooper & Schindler, 2006; Ghauri & Gronhaug, 2005; Yin, 2014, p. 19; Umbach, 2004).

The hypotheses in this study have been thoroughly tested, and the concepts have been validated by esteemed researchers such as Gefen et al. (2000) and Kline (1998). Both qualitative and quantitative methods were used to operationalize and validate the concepts, as discussed in Creswell (2010), Walsham (2006), and Carson & Coviello (1996). The results are presented in detail in Chapters 5, 6, 7, and 8 of the NFC model, along with the theoretical and methodological contributions of the study. Additionally, this chapter explores the management implications and offers suggestions for future research directions.

10.2. Theoretical Contribution

This research focused on the development of a cybersecurity enhancement model called the NFC model, which contributed to the IS literature and, specifically, the DT stream (Ifinedo, 2014; Carlson et al., 2008; Stewart, 2022). Although previous studies have highlighted different aspects that contribute to a successful IS and DT, the attention given to security has been limited (Tashtoush, 2021; Agyaben et al., 2019; Aydiner et al., 2019). The existing literature on IS frequently emphasises the benefits of DT (Tashtoush, 2021; Agyaben et al., 2019; Ayinder et al., 2019), implying that research on IS security is sparse and there are insufficient security models to address the current cyber threats challenges of DT and IS. While corporate security culture has had huge attention (Safa et al., 2015; Pavlov & Karakaneva, 2011; Safa et al., 2016; Ifinedo, 2014; Stewart, 2021; Hoffmann, 2016; Safa et al., 2016; Ifinedo, 2014; Carlson et al., 2008; Pavlov & Karakaneva, 2011; Ali et al., 2013; Pavlov & Karakaneva, 2011; ISO/IEC, 2013), the significance of security initiatives towards the IS and DT is not yet widely recognised. Companies tend to include enterprise security strategies in IS and DT strategies, believing that this should improve the security of digital products and services, leading to complexity and shortcomings (Safa et al., 2015; Pavlov & Karakaneva, 2011). Thus, conventional IS researchers view security as a burden (Carlson, 2015).

This research contributed to a more holistic cybersecurity model for improving IS and DT strategy by addressing the perspectives of technology, humans, processes, consumers, cybersecurity maturity, digital products/services, and expanding the organisational and relational view to a holistic view of security by incorporating pertinent management-level elements such as commitment, investment, communication, and the efficacy of security awareness training. As a result, this research contributed to the theoretical development of a cybersecurity model for IS and DT (Ande et al., 2020; Jonathan, 2019).

This study also considered that different qualities are required to improve DT and IS cybersecurity (Terglav et al., 2016; Singh & Hess, 2017; Stewart, 2022). These qualities led to a holistic view of an organisation's overall security posture by considering technology, human factors and processes and prioritising application security initiatives, including how, what, when, what, and why. Hence, this study concentrated on analysing the holistic security posture rather than value creation (Soomro, 2016; Terglav et al., 2016; Singh & Hess, 2017; Hassan et al., 2015).

While the traditional security models and standards of information security management systems in the literature are informative to improve the security culture in organisations, this research relied on a holistic approach to analyse the security challenges of organisations during DT. It provided a holistic

cybersecurity model called NFC to efficiently, effectively and consistently address these challenges and provide managers with an implementation strategy to strengthen cybersecurity in this transition due to the evolving cyber threat to IS, which has gained prominence in science and government policy and is a priority for all organisations (Hu, et al., 2011; Karjalainen et al., 2019; Flowerday, 2016).

As mentioned in section 2.7.1, humans are still the weakest link in cyber security. This research has shown that organisations that rely on technical solutions without considering human factors create a gap in the human-technology relationship (Safa et al., 2015; Pavlov & Karakaneva, 2011; Safa et al., 2016; Ifinedo, 2014; Stewart, 2021; Hoffmann, 2016; Safa et al., 2016; Ifinedo, 2014; Carlson et al, 2008; Pavlov & Karakaneva, 2011; Ali et al, 2013; Pavlov & Karakaneva, 2011; ISO/IEC, 2013). As humans and technology interact, they form a system that increases the complexity of cybersecurity challenges (Holgate et al., 2012; Mujinga et al., 2017; Paja et al., 2015; Davis et al., 2014), and this is where the NFC model facilitates cybersecurity initiatives by reducing the risk of overlooking complexity or taking a system level for granted.

In the IS field, there is extensive research on how companies within industries can improve their digital security through various management strategies. However, empirical evidence on how key management factors can impact digital security at the cybersecurity level is lacking (Dhillon, 2021; Mahfuth et al., 2017; Moeini et al., 2017). Many studies focus on the organisational perspective of innovation and pay little attention to the maturity of cyber threat intelligence (Stewart, 2022; Provan & Milward, 1995). Furthermore, previous measures and definitions of digital security have focused on organisational antecedents and outcomes rather than appropriate metrics for security.

To address these gaps, a recent study aimed to improve cybersecurity in the context of IS, DT, and the entire organisation. Rather than incentivising innovation, this study aimed to secure digital products and services. The researchers reviewed prior literature to identify relevant constructs, conducted qualitative research to confirm their applicability, and developed metrics that were validated both qualitatively and quantitatively. The study focused on key constructs such (i) security misperception, (ii) threat vulnerability and risk assessment, (iii) cybersecurity strategy, (iv) secure IS engineering, (v) security audit and assessment, (vi) protection monitoring, (vii) strategic advanced threat intelligence, (viii) incident response and remediation, (ix) managers and stakeholders, (x) information security investment, (xi) cyber security investment, (xii) information security policy, (xiii) application security policy, (xiv) information security facilitators, (xv) security training, (xvi) commitment, and (xvii) external

partners (Stewart, 2022). The tested model also contributed to the theoretical improvement of the IS and DT cybersecurity analysis layer.

10.3. Methodological Contribution

The lack of empirical studies on an appropriate cybersecurity model to improve security measures for IS and DT is partly due to the methodological challenges posed by the problems of defining the key components that need to work together effectively.

Quantitative Research at the Cybersecurity Level of Analysis

Empirical studies of cyber threats in IS and DT can be problematic. Previous empirical studies have paid little attention to security in these two areas (Ong et al., 2018; Ferreira et al., 2020; Soto-Acosta, 2018). Confidentiality, integrity, and availability are the three core components of the CIA triad, an information security model that guides an organisation's security procedures and policies (Ifinedo, 2014; ISO/IEC, 2013). The few studies that have explored cybersecurity in this CIA context have focused exclusively on confidentiality, integrity, or availability and have not addressed all three areas simultaneously. Those that have addressed the three areas simultaneously have also ignored non-repudiation and authenticity, and those that have addressed non-repudiation and authenticity have also ignored the CIA. This inadequacy of the literature and proposed models creates problems and requires more resources, time, and costs to implement and maintain. In addition, the security of the applications and software that enable this transition is often neglected (Stewart, 2022). Some have primarily taken a focal organisational viewpoint and defined the perimeters of security approaches on an ego-centric basis, confined to the relationships of a focused organisation (Provan & Milward, 1995).

Nonetheless, few existing studies incorporate the perspectives of different types of industry participants. However, their proposed remedies could be more adaptable, scalable, and holistic to address DT enablers' cybersecurity challenges and improve the security landscape of all industries (Leseure et al., 2001). This study thus contributed to a novel methodology that enabled empirical testing at the level of cybersecurity analysis by combining qualitative and quantitative research.

The qualitative research used key informant interviews, snowballing and triangulation to gain initial knowledge of security constraints (Cooper & Schindler, 2006; Ghauri & Gronhaug, 2005; Yin, 2014, p. 19; Umbach, 2004). Focusing on a particular sector was crucial to ensure that the interviewees and the researcher had a mutual frame of reference (Marsden, 1990b). The sector organisations' profile was identified by interviewing key informants from the industry until a common understanding of the key

participants was established (Perry & Rao, 2007). These findings were also triangulated using data on collaboration acquired from other governmental and industrial reports. As a result, the snowballing strategy was used in this study to identify specific informants from partner organisations (Blaxter et al., 2001). Given the interconnectivity of the sectors, this was deemed an effective way for more precisely defining population borders (Sarantakos, 1998). Since interconnectedness is a key feature of sectors, approaches based on random sampling and unit independence may be deemed inadequate (Brito, 1999).

Extensive quantitative fieldwork was conducted with the organisations in the above industries. Multiple informants were interviewed to increase the reliability of each organisation's responses (Marsden, 1990b; Cooper & Schindler, 2006; Ghauri & Gronhaug, 2005; Yin, 2014 p. 19; Umbach, 2004). Respondents were asked to indicate the organisations they worked with to give them more flexibility. This helped us identify new participants to include in the study (Marsden, 1990b; Wasserman & Faust, 1995).

In defining the security concerns and identifying respondents, the mix of qualitative and quantitative methods, snowballing and triangulation with secondary reports proved beneficial. The large number of respondents from each organisation contributed to the increased trustworthiness of the research.

10.4. Managerial Implications

This research provides recommendations to diverse stakeholders, including individuals from various industries. Table 5 highlights the essential elements necessary to enhance cybersecurity in DT and IS, which may interest organisations.

Table 5. Key constructs & variables to strengthen cybersecurity

Key Factors	Implications
Managers' security support and commitment (Whitman & Mattord, 20014; Ifinedo, 2014; Stewart, 2021; Stewart & Jürjens, 2017; ISO/IEC, 2013)	<ol style="list-style-type: none"> 1. Top management should promote, commit to, and acknowledge the significance of information security. 2. Top management must have clear instructions for protecting information security assets from incidents such as information security breaches by unauthorised persons.

	<ol style="list-style-type: none"> 3. Top management security awareness is crucial for an effective information security system. 4. Top management involvement and accountability and setting parameters for the information security programme can help protect the company's assets.
<p>Invest in security programs (Stewart & Jürjens, 2017; Stewart, 2022; 2022)</p>	<ol style="list-style-type: none"> 1. Managers must invest in Cybersecurity Threat Intelligence to equip their businesses with robust defences that protect their employees and customers from ransomware and phishing attacks and keep their confidential data safe. 2. In the worst case, cyber-attacks or security breaches can devastate a company. Therefore, cyber security should be high on the agenda of the company's management and board of directors.
<p>Implement in-depth security measures (Whitman & Mattord, 2009; Ifinedo, 2014; Stewart, 2021; Stewart & Jürjens, 2017; ISO/IEC, 2013)</p>	<ol style="list-style-type: none"> 1. Implementing information security measures will only succeed with the commitment and support of top management. 2. Top management must effectively sensitise all employees to end-user security.
<p>Foster security culture and trust (Stewart, 2018; Stewart, 2017)</p>	<ol style="list-style-type: none"> 1. Trust is a decisive factor for the success of a DT. An essential component of trust is confidence in an institution, i.e., the individual's conviction that the platform they are trading is safe. 2. Trust is a multi-dimensional, complex mechanism vital to business relationships. 3. In addition, Information Security components such as confidentiality, integrity, availability, authentication, accountability, security, privacy, and authorisation have the potential to influence trust convictions and intentions in a significant way. 4. Top management must reward employees for their contribution to a positive security culture.

<p>Foster security culture during application development (Whitman & Mattord, 2009; Ifinedo, 2014; Stewart, 2021; Stewart & Jürjens, 2017; ISO/IEC, 2013)</p>	<ol style="list-style-type: none"> 1. Top management must create simple, transparent application security policies. 2. They should invest in training software engineers and system administrators. 3. Top management must provide software engineers and system administrators with security training. 4. Top management must make information security a corporate priority. 5. Managers are responsible for ensuring that a security team is involved in project change management and software development life cycle (SDLC).
<p>Improve security awareness training (Whitman & Mattord, 2009; Ifinedo, 2014; Stewart, 2021; Stewart & Jürjens, 2017; ISO/IEC, 2013)</p>	<ol style="list-style-type: none"> 1. Training and awareness-raising of managers, department heads and employees are crucial for effective IS and DT security management. 2. The effectiveness of the information security policy and compliance, responsibility for information security, and information security guidelines are crucial for effective IS and DT security management.
<p>Implement and foster ISP (infosec) (Whitman & Mattord, 2009; Ifinedo, 2014; Stewart, 2021; Stewart, 2022; Stewart, 2022; Stewart & Jürjens, 2017; ISO/IEC, 2013; Maynard & Ruighaver, 2006; Ølnes, 1994; Siponen, 2014; Stahl et al., 2012)</p>	<ol style="list-style-type: none"> 1. A strategic ISP and compliance must be implemented and promoted by managers. 2. Managers must influence staff in designing and promoting compliance with the ISP. 3. Regular and direct communication between managers and staff is crucial for educating them about the ISP. 4. Integrating various security components and initiatives offered by a security architecture, which includes humans, procedures, and technology, can be complex. Therefore, management must support a framework to manage this complexity.

To improve their cybersecurity maturity level, industry players should distribute cyber threat intelligence (CTI) more balanced while respecting privacy (Ferreira et al., 2014; Yee, 2004; Brewer &

Nash, 1989; Clark & Wilson, 1987; Phelps et al., 2000). Sharing CTI between security operations centres, management, other industrial lines, and employees can enhance security culture—this sharing and collaboration foster CTI maturity (Stewart, 2022). Organisations must collaborate with external partners within the CTI maturity framework to ensure that information is shared across borders (Böhm et al., 2018; Mavroeidis et al., 2017; Zhao et al., 2017; Howard et al., 1998). Proactive managers who recognise the significance of security and the detrimental effects of a data breach on their organisation must enhance the attitudes of humans - the weakest link in the security chain. In addition, managers should be willing to invest in security initiatives and refrain from negligence and mobbing tactics when their laxity in security is pointed out to them, potentially affecting the underlying relationships. Coordinating security programs effectively without being too inflexible or limiting is essential. Formalisation is necessary to achieve this. The achievement of cybersecurity objectives within the contexts of information systems and digital technology requires a unified organisation. Security is a shared obligation between all of us.

To create a security culture and secure IS and DT, leaders should actively recognize the need to participate in security initiatives from the outset. By implementing these initiatives, managers can approve and support security projects, proactively approach DT agendas, and swiftly adapt to the results. Proper management training on security can be useful or even fundamental for all stakeholders in the industry to ensure that prudent security practices are well articulated toward promising outcomes.

For DT to be successful, data security, trust, and privacy are key components. Hence, companies should demonstrate trustworthy behaviours, such as keeping their word, being honest and transparent, and behaving reasonably towards their partners and customers. Ensuring confidentiality, integrity, availability, non-repudiation, and authenticity of data, without compromising credibility, through a well-designed security strategy, as recommended in this research, using appropriate measures to improve the security efficiency of IT, IS and DT. To increase efficiency, employees should receive security training based on their value proposition rather than affiliation.

These constructs and variables may help develop methods to deal with problematic situations, including misperception of security by management, inadequate funding for security, inadequate levels of coordination, inconsistent security practices or lack of diligence in information security. These conceptions and conclusions may interest stakeholders in higher education, including ICT and DT

agencies, in undertaking similar efforts. Furthermore, companies in the field of innovation can utilise the research to comprehend better the key components necessary for a successful cybersecurity plan.

10.5 Discussion

This thesis is based on six published papers. The first paper focused on answering three research questions: What are the barriers to adopting FinTech innovations? Do customers value the benefits of FinTech more than data security? How important is data security and trust in FinTech? The study used the NFC model to create a "FinTech adoption" model and identify specific challenges and impacts hindering FinTech adoption. The model was validated through an online survey of 209 mobile phone users. The study found that while the number of mobile users is increasing, the adoption of FinTech is sluggish. Interestingly, almost all respondents (99%) have mobile devices, but only a small % (10%) know FinTech. Additionally, only 10 out of 209 respondents have ever used FinTech services, which is less than 1% of the respondents. This paper concluded that, there is a significant discrepancy between mobile device ownership and the awareness and acceptance of FinTech services. This presents a clear opportunity for FinTech incubators and banks to improve security measures and promote digital trust among potential customers. The study emphasises the need to understand the key factors influencing FinTech adoption, which is essential for players in the financial technology sector who want to expand their presence in the global market. The study provides a valuable basis for future research and projects to improve the status of FinTech and reduce the adoption gap.

The second paper focused on answering three research questions: What is the connection between the factors that cause the challenges in the IaaS implementation model in financial sectors? Can data security and consumer trust help improve the performance of IaaS strategies and enable banks to achieve economies of scale for global intensity? To what extent are data security and consumer trust important in the context of IaaS? The study used the NFC model to create a model of "IaaS adoption" and identify specific challenges and impacts hindering IaaS adoption. The model was validated through an online survey of 208 bank employees. The study found that the financial sector faces numerous obstacles and challenges in adopting cloud computing technology. This is due to the industry's high level of regulation and sensitivity to security concerns. Regulatory compliance is a significant barrier to adopting cloud computing in the financial sector. Strict national and European regulations, such as the General Data Protection Regulation (GDPR) and Federal Financial Supervisory Authority (BaFin) guidelines, place obligations on financial institutions regarding handling customer data and financial transactions. Using cloud services becomes a challenge, especially when the data is stored in another

country, as these regulations impose strict guidelines that must be followed. Due to the sensitive nature of the financial industry, security and privacy are paramount. As a result, many financial institutions are hesitant to adopt cloud computing due to concerns about confidentiality, integrity, invasion of privacy, availability of data, and data breaches. To advance the usage of cloud computing in the financial sector, cloud service providers need to work closely with financial institutions to provide solutions that meet their regulatory requirements, data security needs, and operational preferences. Financial institutions need to invest in robust cybersecurity measures to ensure that cloud services are secure and compliant, which can help address the challenges and promote the benefits of cloud computing in the financial industry.

Achieving security and compliance is crucial in information security, particularly when adhering to industry standards. The third paper exploring the link between industry standards compliance and application security provides insight into how these factors affect each other. The study focuses on the impact of industry standards compliance on application security. The study found that application security is a significant concern in the digital era, as cyberattacks frequently target applications. Security breaches and other incidents can occur as a result of vulnerabilities in applications. Application security must be ensured to protect sensitive data and maintain the trust of customers and stakeholders. The study suggests that compliance with industry standards is insufficient to ensure adequate application security. In short, while industry standards are an essential starting point, additional measures are needed to ensure a high level of application security, as compliance with standards can only address specific security concerns, including privacy and access control.

The study may highlight the need for organisations to implement application-specific security measures beyond what is mandated by compliance standards. This could include secure coding practices, regular security assessments, and the use of security tools and technologies designed to identify and mitigate application vulnerabilities. The dynamic nature of the threat landscape is a significant factor. Compliance standards are typically static and may not adapt quickly to emerging threats and vulnerabilities. Application security must remain flexible and responsive to changing attack vectors and techniques. Application security is an ongoing process that requires continuous monitoring and improvement. Compliance is often a point-in-time assessment, and organisations may mistakenly assume they are secure after achieving compliance. The study may encourage a culture of continuous security improvement.

The findings of the study may underscore the importance of striking a balance between compliance and security. Compliance should serve as a foundation, but organisations should go beyond compliance requirements to build a robust security posture. They can use compliance as a baseline and implement additional security controls that are specific to their applications and potential threats. The study might also highlight the value of collaboration and information sharing within industries. Organisations can benefit from sharing best practices and insights related to application security to collectively enhance security measures.

In conclusion, an empirical study on the impact of industry standards compliance on application security should provide valuable insights into the relationship between compliance and security. It likely underscores the need for a holistic approach, where compliance serves as a foundation, but organisations must proactively address application-specific security challenges to effectively protect their assets in an ever-evolving threat landscape.

The fourth paper focused on answering two research questions: What are the current gaps in past literature on IS/IT strategy that contribute to the biggest challenges for companies in DT when it comes to security? What are the elements that are most effective and successful in contributing to the security of a company's DT? This research delves into the questions that can help organisations develop and implement a secure digital strategy. The study analysed and evaluated eight constructs using the NFC model to ensure digital strategy security. It included a comprehensive examination of the current state of digital strategy security and the reasons behind its success or failure. By reviewing the literature, the study identified the most critical factors for IS security, which can assist organisations in making informed decisions. The primary obstacle to embedding security in strategic DT is the misconception of security among leaders in an organisation, which leads to ignorance of security among employees and affects the culture of security.

The fifth paper focused on answering the following research questions: Do the organisations' management boards lack the skills to plan, train, and direct human activities toward security awareness? What are the beliefs of employees regarding the outcomes of information security violations and how such violations affect information security management? What kind of compliance guidance for information security do organisations need to adopt, and on what essential points should this guidance focus? Is there any interrelation between technology and human factors that work together for the successful deployment and implementation of information security management in an organisation? After conducting three surveys and research, NFC was used to improve information

security management in the organisations in this study. This model identified human behaviours and security-related IT issues, which led to better information security management in organisations. In addition, the study found that the factors involved in this model work together, rather than independently, to bridge the gap between technology and humans.

The research question on paper six revolved around creating and executing a successful ISP based on the NFC model. The NFC framework combined six constructs, latent variables, and factors from previous research models to enhance ISP development and compliance within a multinational organisation. The research approach to validate the NFC model yielded positive results and confirmed its practicality. The proposed framework helps to analyse the crucial elements of an ISP development program and can be used to understand the reasons behind the success or failure of current ISPs. As suggested, having a systematic approach is a significant contribution to the development of this field.

The NFC model proposed in this study is a tool for managing cybersecurity in information systems. It covers three stages: situational awareness, control integration, and gap closure. By classifying data into constants and latent variables and subjecting it to a process, the proposed model can significantly enhance its performance within a reasonable timeframe. It can be incorporated into an organisation's security governance, IS security strategy, or DT initiatives.

The proposed model combines cross-functional departments to identify challenges in a mixed environment, including technology, humans, and processes. Before adopting the NFC model, organisations must assess their situational awareness to obtain holistic data for good process performance. This data can then be used to determine the model's appropriate constructs or latency variables. The ultimate goal is to create an accurate model that aligns with organisational objectives.

The study provides key theoretical implications for the broader IS research field by highlighting the evolving role of cybersecurity in modern organisational scopes (Aydiner et al., 2019; Ferreira et al., 2014). It also contributes to a more in-depth knowledge of the DT-security relationship. It creates a theoretical model for researchers to explore the dynamic relationship between cybersecurity behaviours and technological acquisition (Wang et al., 2008)..

In summary, DT presents both security challenges and opportunities for greater efficiency, innovation and competitiveness. Organisations must take a proactive, all-encompassing approach to cybersecurity that includes implementing sound policies, conducting regular risk assessments, and incorporating security into every facet of their digital projects. For secure and effective digital transformation, these

issues must be addressed through a holistic approach to overcome these security challenges. This includes employee training, proactive risk management, regular security assessments, and adherence to industry best practices and compliance standards. To maximise security risks and leverage the benefits of DT, security must be placed at the centre of these initiatives.

10.6 Limitations and future research

To properly analyse the research findings, we need to consider some limitations. The sample sizes of papers one through six were small, ranging from 200 to 733 participants. It would be advantageous to increase the sample sizes used in the study for more precise results. While this study provides a practical and innovative method for collecting industrial data, future research should focus on assessing the consistency and accuracy of responses across various types of organisations, such as academic institutions, corporations, and government entities. Subgroup analysis based on linkage size would also be advantageous, but the small sample size in this study made it impractical. However, additional related studies with larger samples will be beneficial to this investigation because they will enable fascinating cross-group correlations (Morgan & Krueger, 1998; Bertolino et al., 2014; Appelt and others. Maynard et al., 2014).

To gain further insights, exploring the proposed construct hypotheses and NFC model in industries beyond those examined in this study would be useful. Additionally, since the samples were collected only in Germany, the international validity of the results depends on whether researchers in other countries adopt them (Myers & Newman, 2007). Given that innovation ecosystems and growth levels vary by country, country-specific research is necessary to determine the generalizability of these findings to other cultural contexts (Cohen, 2004). Finally, the ability to analyse multiple levels, including organisational, relational, and industry levels, is a significant benefit of industry research.

This research contributes to the maturity of cybersecurity in IS and DT, which has yet to receive sufficient attention to date. However, following previous multi-level studies, future research could combine different levels of analysis and their interrelationships to provide empirical insights into success factors that ensure that a deep security strategy is holistically integrated into such innovations. Nevertheless, this study is a first step towards validating key constructs and using NFC to explore the relationships between them from the perspective of different participants to provide an effective, acceptable, and consistent solution. The results thus contribute to a better understanding of cybersecurity improvement in the light of the IS and DT.

10.7 Chapter Summary

This study is unique in its contribution to Information Systems and Digital Technology. It takes a multidisciplinary approach to enhance cybersecurity from an industry perspective. The study uses relevant literature to build a conceptual model and operational metrics. Qualitative research helped to develop the model, while quantitative research provides empirical support to understand IS strategy and DT security. The study identifies key success factors for enhancing cybersecurity, such as misconceptions among managers, cybersecurity investment, and trust and commitment.

By introducing a new cybersecurity model called NFC and using the appropriate technique to conduct reliable quantitative research in the industries covered by this thesis, the research offers methodological advances in addition to its theoretical contribution. It addresses the borderline challenge, a hypothetical industry concept, and recent debates. To create and confirm scales, a comprehensive review of the existing literature is conducted. The analysis focuses on three key sectors - finance, automobile, and fintech - to identify common patterns that validate the hypothesis and provide insight into industry-specific factors.

Many players in the innovation sector urged businesses to think about the implications. Numerous companies, governmental agencies, academic institutions, and research centres can improve their DT and IS strategies using the study's findings.

As DT becomes widespread and cyber-attacks become sophisticated, there is a need for further research at the industrial level of analysis. This research should include appropriate scales and methodologies to gain deeper insights into this previously under-researched perspective.

10.8 References

- Abir M'baya, Jannik Laval, Nejib Moalla, "An assessment conceptual framework for the modernization of legacy systems", 2017 11th International Conference on Software, Knowledge, Information Management and Applications (SKIMA), pp.1-11, 2017
- Abualoush, S.H., Obeidat, A.M., Tarhini, A., Al-Badi, A. (2018), "The role of employees' empowerment as an intermediary variable between knowledge management and information systems on employees' performance," VINE J. Inf. Knowl. Manag. Syst., vol. 48, no. 2, pp. 217–237, 2018
- Alhabeeb, M., Almuhaideb, A., Le, P., & Srinivasan, B. (2010). Information Security Threats Classification Pyramid. 24th IEEE International Conference on Advanced Information Networking and Applications Workshops. doi:10.1109/WAINA.2010.39
- Alhogail, Areej; Mirza, A. (2014), "A framework of information security culture change", Journal of Theoretical and Applied Information Technology, 64(2), 540-549.
- Ande, R., Adebisi, B., Hammoudeh, M., Saleem, J. (2020)," Internet of Things: Evolution and technologies from a security perspective", Sustainable Cities and Society 54, 101728. <https://doi.org/10.1016/j.scs.2019.101728>.
- Andriotis, P., Oikonomou, G., & Mylonas, A. & Tryfonas, T. (2015), "A Study on Usability and Security Features of the Android Pattern Lock Screen", Information and Computer Security. 24. 10.1108/ICS-01-2015-0001.
- Angelini, M, N. Prigent, and G. Santucci. Percival: proactive and reactive attack and response assessment for cyber incidents using visual analytics. In 2015 IEEE Symposium on Visualization for Cyber Security (VizSec), pp. 1–8. IEEE, 2015.
- Applegate, D. S., & Stavrou, A. (2013). Towards a cyber conflict taxonomy. 5th International Conference on Cyber Conflict. IEEE Xplore Digital Library.
- Arbanas, K., & Hrustek, N. Ž. (2019), "Key Success Factors of Information Systems Security", Journal of Information and Organisational Sciences, 43(3), 131-144.
- Arthur, K., & Olivier, M. (2017). Applying The Biba Integrity Model to Evidence Management. IFIP International Conference on Digital Forensics (pp. 1-15). Pretoria: National Centre for Forensic Science.

- Arun, R., Suresh, V., Madhavan, C. V., and Murthy, M. N. (2010), "On Finding the Natural Number of Topics with Latent Dirichlet Allocation: Some Observations," Pacific-Asia Conference on Knowledge Discovery and Data Mining: Springer, p. 391-402.
- Aydiner, A.S., Tatoglu, E., Bayraktar, E., Zaim, S. (2019), "Information system capabilities and firm performance: Opening the black box through decision-making performance and business-process performance," *Int. J. Inf. Manag.*, vol. 47, pp. 168–182.
- Ayewah, N., Hovemeyer, D., Morgenthaler, J. D., Penix, J. & Pugh, W. (2008), "Experiences using static analysis to find bugs", *IEEE Software*, 25:22–29, Special issue on software development tools, September/October (25:5).
- B. McGuinness and J. L. Foy. A subjective measure of SA: The crew awareness rating scal (cars). In *Proceedings of the first human performance, situation awareness, and automation conference*, Savannah, Georgia, USA, October 2000.
- Bakar, H.A.; Razali, R.; Jambari, D.I. Legacy Systems Modernisation for Citizen-Centric Digital Government: A Conceptual Model. *Sustainability* 2021, 13, 13112. [CrossRef]
- Baskerville, R., 1988. *Designing Information Systems Security*. John Wiley & Sons, New York.
- Baskerville, R. (1999). Investigating Information Systems with Action Research. *Communications of the Association for Information Systems*, 2, pp-pp. <https://doi.org/10.17705/1CAIS.00219>
- Bekkhuss, R. (2016). Do KPIs used by CIOs decelerate digital business transformation? The case of ITIL. Paper presented at the Digital Innovation, Technology, and Strategy Conference, Dublin, Ireland. In the *Proceedings of DIGIT 2016*. <https://aisel.aisnet.org/digit2016/16>
- Bell, D. E. (1973). *Secure Computer Systems: Mathematical Foundations*, Bedford. Bedford, MA: MITRE.
- Bertolino, A., Traon, Y. L., Lonetti, F., Marchetti, E. & Mouelhi, T. (2014), "Coverage based test cases selection for XACML policies" In 2014 IEEE Seventh International Conference on Software Testing, Verification and Validation, Workshops Proceedings, March 31 - April 4, 2014, Cleveland, Ohio, USA, pages 12–21. IEEE Computer Society.
- Bezeley P. *Qualitative Data Analysis with NVivo*. London: Sage; 2007. [Google Scholar]
- Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. *MIS Quarterly*, 37(2),471-482.

- Biba, K. J. (1977). Integrity considerations for secure computer systems. Bedford, Massachusetts: ESD-TR.
- Bishop, J.B., Bauer, K.W. & Becker, E.T. (1998), "A survey of counseling needs of male and female college students", *Journal of College Student Development*, 39, (2), 205-210.. *Journal of College Student Development*. 39. 205-210.
- Blei, D.M., Ng, A.Y., Jordan, M.I. (2003), " Latent Dirichlet Allocation", *Journal of Machine Learning Research* 3:Jan, 993–1022.
- Blohm, M. (2007), 'the influence of interviewers' contact behavior on the contact and cooperation rate in face-to-face household surveys', *International Journal of Public Opinion Research*, 19 (1), pp.97-111.
- Bodeau, D., McCollum, C., Fox, D., 2018. Cyber Threat Modeling: Survey, Assessment, and Representative Framework. The Homeland Security Systems Engineering and Development Institute, The MITRE Corporation.
- Böhm, F., Menges, F., Pernul, G. (2018), "Graph-based visual analytics for cyber threat intelligence", *Cybersecurity*. 1. 10.1186/s42400-018-0017-4.
- Bompard, E., Huang, T., Wu, Y., & Cremenescu, M. (2013). Classification and trend analysis of threats origins to the security of power systems. *Electrical Power and Energy Systems*, 50, 50–64. doi:10.1016/j.ijepes.2013.02.008
- Brewer, D. F., & Nash, M. J. (1989). The Chinese wall security policy. *IEEE Symposium on Security and Privacy*, (pp. 1-13). Oakland, CA.
- Britten, N. (1995), "Qualitative Interviews in Medical Research", *BMJ (Clinical research ed.)*. 311. 251-3. 10.1136/bmj.311.6999.251.
- Bullée, J. W., Junger, M. (2020). "Social Engineering". 10.1007/978-3-319-90307-1_38-1.
- Burns, N. & Grove, S. K. (2001), "The practice of nursing research: Conduct, critique, and utilization". Philadelphia, PA: Saunders.
- Byrne, B. (2001) *Structural Equation Modeling With AMOS: Basic Concepts, Applications, and Programming*, New Jersey, Lawrence Erlbaum Associates, Inc., Publishers.

- Cao, J., Xia, T., Li, J., Zhang, Y., Tang, S. (2009), "A Density-Based Method for Adaptive LDA Model Selection", *Neurocomputing* 72 (7–9), 1775–1781.
- Charitoudi, K., & Blyth, A. (2013), "A Socio-Technical Approach to Cyber Risk Management and Impact Assessment", *Journal of Information Security*, 4(1), 33-41.
- Chen, S.P. and Redar, J.M. (2014), "Ageing workforce knowledge management and transactional and transformational leadership: a socio-technical systems framework and a norwegian case study", *International Journal of Business and Social Science*, Vol. 5 No. 5, pp. 11-2
- Cheng, E.C., 2000. An object-oriented organisational model to support dynamic role-based access control in electronic commerce. *Decision Support Systems* 29 (4), 357–369.
- Chooi, S.T & Ahmad, K.M. 2017(" National cybersecurity strategies for digital economy. In 2017 International Conference on Research and Innovation in Information Systems (ICRIIS), pages 1–6. IEEE, 2017.
- Chu. M, K. Ingols, R. Lippmann, S. Webster, and S. Boyer. Visualizing attack graphs, reachability, and trust relationships with navigator. In *Proceedings of the Seventh International Symposium on Visualization for Cyber Security (VizSec)*, pp. 22–33, 2010
- Churchill, G. A. (1979) 'A Paradigm for Developing Better Measures of Marketing Constructs'. *Journal of Marketing Research*, Vol.16 No.1, pp.64-73
- Clark, D. D., & Wilson, D. R. (1987). A Comparison of Commercial and Military Computer Security Policies. *Proceedings of the 1987 IEEE Symposium on Research in Security and Privacy* (pp. 184–193). Oakland, CA: IEEE Press.
- Collet. S (2020), "What is security's role in digital transformation?"
<https://www.csoonline.com/article/3512578/what-is-securitys-role-in-digital-transformation.html>, 2020. [Online; accessed 23-September-2022].
- Creswell, J. W. (1998). *Qualitative inquiry and research design: Choosing among five traditions*. Sage Publications, Inc
- Creswell, J. W. (2010). *Projeto de pesquisa: métodos qualitativo, quantitativo e misto [Research design: Qualitative, quantitative, and mixed methods approaches]* (3rd ed). Trad. Magda Lopes, Rev. téc. Dirceu da Silva. Porto Alegre, Brazil: Artmed.

- Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future Directions for Behavioral Information Security Research," *Computers & Security* (32:2013), pp. 90- 101.
- Cully, M., Woodland, S., O'Reilly, A. and Dix, G. (1999), *Britain at Work: As Depicted by the 1998 Workplace Employee Relations Survey*. London, Routledge.
- Da Veiga, A., Martins, N. (2015), "Improving the information security culture through monitoring and implementation actions illustrated through a case study," *Computers & Security*, vol. 49, pp. 162–176.
- Davidson, C. (2009). Transcription: Imperatives for qualitative research. *International Journal of Qualitative Methods*, 8, 1–52. <https://doi.org/10.1177/160940690900800206>
- Davis, M.C., Challenger, R., Jayewardene, D.N.W. and Clegg, C.W. (2014), "Advancing socio-technical systems thinking: a call for bravery", *Applied Ergonomics*, Vol. 45 No. 2, pp. 171-180
- Dempsey, K., Chawla, N.S., Johnson, A., Johnston, R., Jones, A.C., Orebaugh, A., Scholl, M., Stine, K.: NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organisations. Tech. rep. (2011)
- Denzin, N., & Lincoln, Y. (2000). The discipline and practice of qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (pp. 1–32). Sage
- Deveaud, R., SanJuan, E., Bellot, P. (2014), "Accurate and Effective Latent Concept Modeling for Ad Hoc Information Retrieval. Document numérique 17 (1), 61–84. Dhillon, G. (Ed.), 1997. *Managing Information System Security*", Macmillan Education UK, London.
- DeWitt, A. & Kuljis, J. (2006), " Aligning usability and security: A usability study of polaris", *ACM International Conference Proceeding Series*. 149. 1-7. [10.1145/1143120.1143122](https://doi.org/10.1145/1143120.1143122).
- Dhillon, G., Backhouse, J. (2001), " Current Directions in Is Security Research: Towards Socio-Organisational Perspectives", *Information Systems Journal* 11 (2), 127–153.
- Dhillon, G., Oliveira, T., Susarapu, S., & Caldeira, M. (2016), "Deciding between information security and usability", *Developing value based objectives. Computers in Human Behavior*. 61. 656-666. [10.1016/j.chb.2016.03.068](https://doi.org/10.1016/j.chb.2016.03.068).

- Dhillon, G., Smith, K., & Dissanayake., I. (2021), "Information systems security research agenda: Exploring the gap between research and practice", *The Journal of Strategic Information Systems*. 30. 10.1016/j.jsis.2021.101693.
- Disterer, G. (2013) ISO/IEC 27000, 27001 and 27002 for information security management. *J Inform Security* 4(2):92–100
- Doukidis, G., Spinellis, S., & Ebert, C. (2020), "Digital transformation-a primer for practitioners", *IEEE Software*, 37(5):13–21, 2020.
- Duc, A. N., & Chirumamill., A. (2019)," Identifying security risks of digital transformation-an engineering perspective", In *Conference on e-Business, e-Services and e-Society*, pages 677–688. Springer.
- Duc, A.N & Chirumamilla, A (2019). "Identifying Security Risks of Digital Transformation ", *An Engineering Perspective*. 677-688. 10.1007/978-3-030-29374-1_55.
- Eder-Neuhauser, P., Zseby, T., Fabini, J. (2018),"Malware propagation in smart grid monocultures Malware-Ausbreitung in Smart Grid-Monokulturen", *Elektrotechnik and Informationstechnik* 135 (3), 264–269.
- Eisenhardt, K. (1998), 'Building Theories from Case Study Research', *Academy Management Review*, Vol 14 (4), pp.532-550
- Ellström, D., Holtström, J., Berg, E., & Josefsson, C. (2022). Dynamic capabilities for digital transformation. *Journal of Strategy and Management*, 15, 272–286.
- Emery, F.E. (1982),"Sociotechnical foundations for a new social order?",*Human Relations*, Vol. 35No. 12, pp. 1095-1123. No
- Farahmand, F. Navathe, S. B. Sharp, G.P. & Enslow, P. H. (2005). A Management Perspective on Risk of Security Threats to Information Systems. *Information Technology and Management Archive*, 6, 202-225.
- Felderer M et al (2014) Evolution of security engineering artifacts: a state of the art survey. *Int J Secur Softw Eng* 5:48–98
- Ferreira, Ana & Huynen, Jean-Louis & Koenig, Vincent & Lenzini, Gabriele. (2014). A Conceptual Framework to Study Socio-Technical Security. *Lecture Notes in Computer Science*. 10.1007/978-3-319-07620-1_28.

- Ferreira, J., Coelho, A., Moutinho, L. (2020), "Dynamic capabilities, creativity and innovation capability and their impact on competitive advantage and firm performance: The moderating role of entrepreneurial orientation," *Technovation*, vol. 92–93, pp. 1–18, 2020.
- Flowerday, S. V., Tuyikeze, T. (2016), "Information security policy development and implementation: The what, how and who," *Comput. Secur.*, vol. 61, pp. 169–183.
- Fornell, C. & Larcker, D. F. (1981) 'Evaluating Structural Equation Models with Unobservable Variables and Measurement Error'. *Journal of Marketing Research*, Vol.18 No.1, pp.39-50.
- Furnell, S. 2005. "Why Users Cannot Use Security," *Computers & Security* (24:4), pp. 274-279.
- Glaspie, H. W., & Karwowski, W. (2018) "Human factors in Information Security Culture: A Literature Review", *Advances in Intelligent Systems and Computing*, 269-281.
- Gordon, L. A., Loeb, M. P., & Zhou, L. (2011), "The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?", *Journal of Computer Security*, 19(1), 33-56.
- Goudy, W. J. and Potter, H. R. (1975), 'Interview Rapport: Demise of a Concept', *Public Opinion Quarterly*, 39 (4), pp.529-43
- Griffiths, T.L., Steyvers, M. (2004)," Finding Scientific Topics. *Proceedings of the National Academy of Sciences* 101 (suppl 1), 5228–5235.
- Han, D., Dai, Y., Tianlin Han, & Dai, X. (2015), "Explore Awareness of Information Security: Insights from Cognitive Neuromechanism," *Computational Intelligence and NeuroScience* , 1-11.
- Hassan, N. H., Ismail, Z., & Maarop, N. (2015), "Information Security Culture, A systematic Literature Review". *The 5th International Conference on Computing and Informatics* (pp. 456-463).
istanbul: he 5th International Conference on Computing and Informatics.
- Helsloot, I., & Groenendaal, J. (2011), " Naturalistic decision making in forensic science: Toward a better understanding of decision making by forensic team leaders", *Journal of forensic sciences*, 56(4), 890-897.
- Hess, T., Matt, C., Benlian, A., & Wiesböck, F. (2016). Options for formulating a digital transformation strategy. *MIS Quarterly Executive*, 15(2).
<https://aisel.aisnet.org/misqe/vol15/iss2/6>

- Hess, T., Matt C., Benlian, A., Wiesböck, F. (2016), "Options for formulating a digital transformation strategy, *MIS Quarterly Executive*, 15(2).
- Hong, J., Kim, D., 2016. Assessing the effectiveness of moving target defenses using security models. *IEEE Trans. Dependable Secure Comput.* 13 (2), 163–177, <https://doi.org/10.1109/TDSC.2015.2443790>.
- Hong, J.B., Kim, D.S., 2016. Towards scalable security analysis using multi-layered security models. *J. Netw. Comput. Appl.* 75, 156–168, <https://doi.org/10.1016/j.jnca.2016.08.024>.
- Hong, J.B., Kim, D.S., Chung, C.-J., Huang, D., 2017. A survey on the usability and practical applications of graphical security models. *Computer Science Review* 26, 1–16, <https://doi.org/10.1016/j.cosrev.2017.09.001>.
- Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011), "Does Deterrence Work in Reducing Information Security Policy Abuse By Employees?", *Communications of the ACM*, 54(6), 54-90.
- Huang, A.H., Lehav, R., Zang, A.Y., Zheng, R. (2018), "Analyst Information Discovery and Interpretation Roles: A Topic Modeling Approach. *Management Science* 64 (6), 2833–2855.
- Humphreys, E (2011) Information security management system standards. *Datenschutz und Datensicherheit* 35(1):7–11
- Introna, L. D. & Wood, D. (2004), "Picturing algorithmic surveillance: The politics of facial recognition systems". *Surveillance & Society*, 2, 177-198.
- ISO/IEC: ISO/IEC 27001:2013: Information technology – Security techniques – Information security management systems – Requirements (2013). URL <http://shop.bsigroup.com/ProductDetail/?pid=00000000030313534>
- ISO/IEC: ISO/IEC 27005:2011: Information technology – Security techniques – Information security risk management. Tech. rep., ISO/IEC (2011)
- ISO/IEC. 27000:2018, "Information technology—Security techniques—Information security management systems—Overview and vocabulary", 2018.
- ISO/IEC. 27001:2013, "International standard ISO/IEC Information technology—Security techniques—Information security management systems—Requirements", vol. 2013, 2013.

- ISO/IEC. 27002:2013, "Information technology—Security techniques—Code of practice for Information security controls", 2013.
- ISO/IEC. 27017:2015, "Information technology—Security techniques—Code of practice for information security controls based on ISO/IEC 27002 for cloud services", 2015.
- ISO/IEC 27032:2012 (E) information technology e security techniques e guidelines for Cyber Security, Geneva, Switzerland:ISO/IEC, 2012.
- ITU. (2017). Global Cybersecurity Index (GCI). Geneva, Switzerland: International Telecommunication Union.
- Jagadamba G, Sharmila S, Gouda T (2014) A secured authentication system using an effective keystroke dynamic. In: *Emerging research in electronics, computer science and technology*, Springer, pp 453–460
- Julian A. García-García, C. Arevalo Maldonado, Ayman Meidan, Esteban Morillo-Baro, María José Escalona, "gPROFIT: A Tool to Assist the Automatic Extraction of Business Knowledge From Legacy Information Systems", *IEEE Access*, vol.9, pp.94934-94952, 2021.
- Kabir, M.E., Wang, H., Bertino, E., 2012. A role-involved purpose-based access control model. *Information Systems Frontiers* 14 (3), 809–822.
- Kane, G. C., Phillips, A. N., Copulsky, J. R., & Andrus, G. R. (2019). *The technology fallacy: How humans are the real key to digital transformation*. Cambridge, Massachusetts: The MIT Press.
- Karjalainen, M., Sarker, S., Siponen, M. (2019.), "Toward a Theory of Information Systems Security Behaviors of Organisational Employees: A Dialectical Process Perspective. *Information Systems Research* 30 (2), 687–704.
- Karjalainen, M., Sarker, S., Siponen, M. (2019)," Toward a Theory of Information Systems Security Behaviors of Organisational Employees: A Dialectical Process Perspective", *Information Systems Research* 30 (2), 687–704.
- Karpunina, E.K., Konovalova, M.E., Shurchkova, Julia, V.S., Isaeva, Ekaterina, A., and Abalakin, A.A. (2019), "Economic security of businesses as the determinant of digital transformation strategy", In *Institute of Scientific Communications Conference*, pages 251–260. Springer.

- Karpunina, E.K., Konovalova, M.E., Shurchkova, Julia, V.S., Isaeva, Ekaterina, A., and Abalakin, A.A. (2019), "Economic security of businesses as the determinant of digital transformation strategy", In Institute of Scientific Communications Conference, pages 251–260. Springer.
- Karumbaiah, S., Wright, R.T., Durcikova, A., Jensen, M. L. (2016), "Phishing training: A preliminary look at the effects of different types of training", In Proceedings of the 11th Pre-ICIS Workshop on Information Security and Privacy, pages 1–10.
- Karumbaiah, S., Wright, R.T., Durcikova, A., Jensen, M. L. (2016), "Phishing training: A preliminary look at the effects of different types of training", In Proceedings of the 11th Pre-ICIS Workshop on Information Security and Privacy, pages 1–10.
- Khalil, F., & Alam, H. M. (2020). Identification of Fintech Driven Operational RiskEvents. Journal of the Research Society of Pakistan, 1(57), 75–87
- Khan, M.; Ali, I.; Nisar, W.; Saleem, M.Q.; Ahmed, A.S.; Elamin, H.E.; Mehmood, W.; Shafiq, M. Modernization Framework to Enhance the Security of Legacy Information Systems. *Intell. Autom. Soft Comput.* 2022, 32, 543–555. [CrossRef]
- Khan, S., and Madnick, S. 2019. "Cybersafety: A System-Theoretic Approach to Identify Cyber-Vulnerabilities & Mitigations in Industrial Control Systems," Available at SSRN 3542551).
- Kline, R. B. (2005) Principles and Practice of Structural Equation Modeling, New York, London, The Guilford Press.
- Knapp ED, Langill JT (2014) Industrial network security: securing critical infrastructure networks for smart grid, SCADA, and other industrial control systems. Syngress, Burlington
- Kordy, B., Wide, W., 2018. On quantitative analysis of attack defense trees with repeated labels. In: International Conference on Principles of Security and Trust. Springer, pp. 325–346.
- Kraemer, S., Carayon, P and Clem, J. (2009), "Human and organisational constructs in computer and information security: Pathways to vulnerabilities," *Comput. Secur.*, vol. 28, no. 7, pp. 509–520.
- Kranz, M., Murmann, L., & Michahelles, F. (2013), "Research in the large: Challenges for large-scale mobile application research: A case study about NFC adoption using gamification via an app store". *IJMHCI*5(1), 45-61. doi:10.4018/jmhci.2013010103.

- Kriaa S, Pietre-Cambaces L, Bouissou M, Halgand Y (2015) A survey of approaches combining safety and security for industrial control systems. *Reliab Eng Syst Saf* 139:156–178
- Krumay B, Bernroider EWN, Walser R (2018) Evaluation of cybersecurity management controls and metrics of critical infra-structures: a literature review considering the NIST Cybersecurity Framework. In: Gruschka N. (ed) NordSec. Lecture Notes in Computer Science, vol 11252, pp 369–384.
- Kumar, D., Sharma, A., Kumar, R., Sharma, N. (2019), "Restoration of the network for next generation (5G) optical communication network", In 2019 International Conference on Signal Processing and Communication (ICSC). IEEE; 2019. pp. 64–8. Search in Google Scholar.
- Kvale, S., & Brinkmann, S. (2009). *Interviews: Learning the craft of qualitative research interviewing* (2nd ed.). London, United Kingdom: Sage
- Lavin, D and Maynard, D. (2001), 'Standardization vs. Rapport: Respondent Laughter and Interviewer Reaction during Telephone Surveys', *American Sociological Review*, 66 (3), pp.453-479
- Legner, C., Eymann, T., Hess, T., Matt, C., Bohmann, T., Drews, P., Madche, A., Urbach, N., Ahlemann, F. (2017), "Digitalization: opportunity and challenge for the business and information systems engineering community", *Bus. Inform. Syst. Eng.* 59 (4), 301–308.
<https://doi.org/10.1007/s12599-017-0484-2>.
- Li, P. L., Amy, J. K., Andrew, B. (2020), "What distinguishes great software engineers? *Empirical Software Engineering*, 25(1):322–352.
- Lubua, E. W., & Pretorius, P. D. (2019), "Ranking Cybercrimes based on their impact to organisations' welfare," *THREAT Conference Proceedings* (pp. 1-11). Johannesburg: THREAT Conference Proceedings.
- Lucila, N. B. (2016), "Information Security Policy Development: A Literature Review," *Int. J. Innov. Res. Inf. Secur.*, vol. 3, no. 4, pp. 1–7.
- Lundgren, B., & Möller, N. (2017). *Defining Information Security. Science and Engineering Ethics*, 25(3), 1-8.
- Lundgren, B., & Möller, N. (2017). *Defining Information Security. Science and Engineering Ethics*, 25(3), 1-8.

- Luo, A., Guchait, P., Lee, L. and Madera, J.M. (2019), "Transformational leadership and service recovery performance: the mediating effect of emotional labor and the influence of culture", *International Journal of Hospitality Management*, Vol. 77 No. 4, pp. 31-39
- Luse, A., Mennecke, B., Townsend, A., Demarie, S. (2013), "Strategic Information Systems Security: Definition and Theoretical Model," *AMCIS 2013*, August 15-17. Chicago, USA.
- M. Endsley. Toward a theory of situation awareness in dynamic systems. In *Human factors Journal*, volume 37(1), pages 32–64, March 1995
- Macpherson, W. G., Lockhart, J. C., Kavan, H., & Iaquinto, A. L. (2015). Kaizen: A Japanese philosophy and system for business excellence. *Journal of Business Strategy*, 36(5), 3-9.
<https://doi.org/10.1108/JBS-07-2014-0083>
- Maedche, A. (2016). Interview with Michael Nilles on "What Makes Leaders Successful in the Age of the Digital Transformation?". *Business & Information Systems Engineering*, 58(4), 287-289.
[doi:10.1007/s12599-016-0437-1](https://doi.org/10.1007/s12599-016-0437-1)
- Maheshwari, R., & Pathak, S. (2012). A Proposed Secure Framework for Safe Data Transmission, in *Private Cloud*. *International Journal of Recent Technology and Engineering*, 1(1), 78–82
- Mahfuth, A., Yussof, S., Baker, A. A., & Ali, N. (2017), "A systematic literature review: Information security culture. *International Conference on Research and Innovation in Information Systems*", (ICRIIS), (pp. 1-6). Langkaw: *International Conference on Research and Innovation in Information Systems (ICRIIS)*, Langkaw
- Marcuschi, L. A. (2007). *Análise da conversação [Conversation analysis]* (6th ed.). São Paulo, Brazil: Ática.
- Masaaki, I. (1986). *Kaizen: The key to Japan's competitive success*. New York, Ltd: McGraw-Hill.
- Matt, C., Hess, T., & Benlian, A. (2015). Digital transformation strategies. *Business & Information Systems Engineering*, 57(5), 339-343.
- Mavroeidis, V., Bromander, S. (2017), "Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence", 10.1109/EISIC.2017.20.
- McAdam, R., Leonard, D., Henderson, J and Hazlett, S. (2008), 'A grounded theory research approach to building and testing TQM theory in operations management', *Omega*, 36 (5), pp.825-37.

- McFadzean, E., Ezingear, J.-N., and Birchall, D. (2006), "Anchoring Information Security Governance Research: Sociological Groundings and Future Directions," *Journal of Information System Security* 2(3), p. 3-48.
- Meraviglia, L. (2018). Technology and counterfeiting in the fashion industry: Friends or foes? *Business Horizons*, 61(3), 467-475.
- Mitnick, K. & Simon, W. L. (2002), "The art of deception: Controlling the human element of security", New York, NY: John Wiley & Sons.
- Moeini, M., Rahrovani, Y. & Chan, Y.E. (2019), "A review of the practical relevance of IS strategy scholarly research", *The Journal of Strategic Information Systems*, 28(2).
- Möller, A., Michahelles, F., Diewald, S., Roalter, L., & Kranz, M. (2012), "U Kranz pdate behaviour in app markets and security implications: A case study in Google play", In: Poppinga B. (ed.), *Proceedings of the 3rd International Workshop on Research in the Large, held in Conjunction with Mobile HCI*, pp. 3-6.
- Morgeson, F. P., Aiman-Smith, L.D., & Campion, M.A. (1997), "Implementing work teams: recommendations from organisational behaviour and development theories," In M.M Beyerlein, D.A. Johnson & S.T. Beyerlein (Eds). *Advances in interdisciplinary studies of work teams* (Vol 4, pp. 1-44). Amsterdam: Elsevier Science & Technology Books.
- Mujinga, Mathias & Eloff, Mm & Kroeze, Jan. (2017). A socio-technical approach to information security.
- Mumford, E. (2006), "The story of socio-technical design: reflections on its successes, failures and potential", *Information Systems Journal*, Vol. 16 No. 4, pp. 317-342.
- Myers, M., and Newman, M. (2007), "The Qualitative Interview in IS Research: Examining the Craft," *Information and organisation* (171), pp. 2-26.
- National Institute of Standards and Technology (NIST): NIST SP 800-53 Rev. 4 Recommended Security Controls for Federal Information Systems and Organisations. U.S. Government Printing Office (2013).
[URLhttp://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final{_}updated-errata{_}05-01-2010.pdf](http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final{_}updated-errata{_}05-01-2010.pdf)

- Neuman, W. L. (2007), "Basics of social research": Qualitative and quantitative approaches(2nd ed.). Boston, MA: Allyn and Bacon.
- Newitt, D. (1996). Beyond BPR & TQM-Managing through processes: Is Kaizen enough? Paper presented at the IEE Colloquium on Beyond TQM and Re-Engineering-Managing Through Process, 31.
- NIST, "Framework for improving critical infrastructure cybersecurity", Version1.1, (2018). [Online].<https://doi.org/10.6028/NIST.CSWP.04162018>
- Noel, S., 2018. A Review of Graph Approaches to Network Security Analytics. Springer International Publishing, Cham, pp. 300–323, https://doi.org/10.1007/978-3-030-04834-1_16.
- Oliveira,T., Thomas, M., Espadanal, M. (2014), "Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors". *Journal of Information & Management*, 51, pp.497–510.
- Ong, J.W., Ismail, H., Yeap, P.F. (2018), "Competitive advantage and firm performance: the moderating effect of industry forces," *Int. J. Bus. Perform. Manag.*, vol. 19, no. 4, pp. 385–407, 2018
- Paananen, H., Lapke, M., Siponen, M. (2020), "State of the Art in Information Security Policy Development", *Computers & Security* 88, 1–14.
- Padayachee, K. (2012), "Taxonomy of compliant information security behavior", *Computers & Security*, Vol 31, No. 2012, pp673-680.
- Page, C. & Meyer, D. (2000) *Applied Research Design for Business and Management*, Sydney, McGraw-Hill Companies, Inc.
- Paja, Elda & Dalpiaz, Fabiano & Giorgini, Paolo. (2015). *Modelling and Reasoning about Security Requirements in Socio-Technical Systems. Data & Knowledge Engineering*. 98. [10.1016/j.datak.2015.07.007](https://doi.org/10.1016/j.datak.2015.07.007).
- Parker, D. B. (1995). 'A New Framework for Information Security to Avoid Information Anarchy', *Information Security — the Next Decade: Proceedings of the IFIP TC11 eleventh international conference on information security, IFIP/Sec '9*, https://doi.org/10.1007/978-0-387-34873-5_13

- Paté-Cornell, M.E., Kuypers, M., Smith, M., Keller, P., 2018. Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies. *Risk Analysis* 38 (2), 226–241.
- Patton, M. Q. (2002). *Qualitative research and evaluation methods* (3rd ed.). Thousand Oaks, CA: Sage
Hossain Shahriar, Kennesaw State University
- Perkin, N., & Abraham, P., (2017). *Building the Agile Business through Digital Transformation*. Kogan Page Publishers.
- Ramani, G. & Kumar, V. (2008) 'Interaction Orientation and Firm Performance'. *Journal of Marketing*, Vol.72 No.1, pp.27-45.
- Rogers, D. L., (2016). *The Digital Transformation Playbook : Rethink Your Business for the Digital Age*. New York: Columbia Business School Publishing.
- Rokkan, A. I., Heide, J. B. & Wathne, K. (2003) 'Specific Investments in Marketing Relationships'. *Journal of Marketing Research*, Vol.40 No.2, pp.210-224.
- Saini, Vineet & Duan, Qiang & Paruchuri, Vamsi. (2008). Threat Modeling Using Attack Trees. *Journal of Computing Sciences in Colleges*. 23.
- Samonas, S., Coss, D. (2014), "The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security", *Journal of Information System Security* 10 (3), 21–45.
- Sandberg H, Amin S, Johansson K (2015) Cyberphysical security in networked control systems: an introduction to the issue. *IEEE Control Syst* 35:20–23
- Sapronov, K. (2020). *The human factors and information security*. Kaspersky
- Sarwenda, B. (2020), "Intellectual capital, business performance, and competitive advantage: An empirical study for the pharmaceutical companies," *QUALITY Access Success J. Manag. Syst.*, vol. 21, no. 175, pp. 103–106, 2020.
- Sasse, M. A., Brostoff, S., and Weirich, D. 2001. "Transforming the 'Weakest Link'—a Human Computer Interaction Approach to Usable and Effective Security," *BT Technology Journal* (19:3), pp. 122-131.
- Sausalito, C. (2020), "Cybercrime To Cost The World \$10.5 Trillion Annually By 2025. New York", *Cybercrimme Magazine*.

- Sax, L. J., Gilmartin S. K. and Bryant A. N. (2003), "Assessing response rates and non response bias in web and paper surveys," *Research in Higher Education*, 44, 4, 409-431.
- Schneier, Bruce, *Attack Trees*, Dr. Dobb's Journal of Software Tools 24, 12(December 1999): 21-29.
- Seongmo. An & Eom, Taehoon & Park, Jong & Hong, Jin & Nhlabatsi, Armstrong & Fetais, Noora & Khan, Khaled & Kim, Dan. (2019). *CloudSafe: A Tool for an Automated Security Analysis for Cloud Computing*. 602-609. 10.1109/TrustCom/BigDataSE.2019.00086.
- Shahri, A. B., & Mohanna, S. (2016), "The Impact of the Security Competency on "Self-efficacy in Information Security" for Effective Health Information Security in Iran", *The Advances in Intelligent Systems and Computing*, 445, 51-65.
- Singh, S. & Hess, T. (2017)," How chief digital officers promote the digital transformation of their companies", *MIS Quarterly Executive*, 16(1).
- Siponen, M., Baskerville, R., Kuivalainen, T. (2005)," Integrating security into agile development methods", In: *Proc. of HICSS*.
- Sohrabi, N., Von Solms, R., Furnell, S., Elizabeth, P., and Africa, S. (2016), "Information security policy compliance model in organisations," *Comput. Secur.*, vol. 56, pp. 1–13.
- Soomro, Z. A., Shah, M. H., and Ahmed, J. (2016), "Information security management needs more holistic approach: A literature review," *Int. J. Inf. Manage.*, vol. 36, pp. 215–225.
- Soto-Acosta, P., Popa, S., Martinez-Conesa, I. (2018), "Information technology, knowledge management and environmental dynamism as drivers of innovation ambidexterity: a study in SMEs," *J. Knowl. Manag.*, vol. 22, no. 4, pp. 824–849, 201
- Souppaya, M., Scarfone, K.: *NIST Special Publication 800-124 Rev. 1 Guidelines for Managing the Security of Mobile Devices in the Enterprise*. NIST special publication p. 30 (2013). DOI 10.6028/NIST.SP.800-124r1
- Steenkamp, J. B. E. M. & van Trijp, H. C. M. (1991) 'The Use of LISREL in Validating Marketing Constructs'. *International Journal of Research in Marketing*, Vol.8 No.4, pp.283-299.
- Steinbart, P.J., Keith, M.J., Babb, J., 2016. Examining the continuance of secure behavior: A longitudinal field study of mobile device authentication. *Information Systems Research* 27 (2), 219–239.

- Stewart, H., and Jürjens, J. (2017), "Information security management and the human aspect in organisations", *Information & Computer Security*, vol. 25, no. 5, pp. 494–534.
<https://doi.org/10.1108/ICS-07-2016-0054>.
- Stewart, H., and Jürjens, J. (2017), "Information security management and the human aspect in organisations", *Information & Computer Security*, vol. 25, no. 5, pp. 494–534.
<https://doi.org/10.1108/ICS-07-2016-0054>.
- Stewart, H., and Jürjens, J. (2018), "Data security and consumer trust in FinTech innovation in Germany", *Information & Computer Security*, vol. 26, no. 1, pp. 109–128.
<https://doi.org/10.1108/ICS-06-2017-0039>.
- Stewart, H. (2020), "Information Technology and Cyber Security Unplugged": The interrelationship between Human Technology and Cyber Crime Today (English Edition), Rohhat LTD" 2020.
- Stewart, H. (2021), "The hindrance of cloud computing acceptance within the financial sectors in Germany", *Information and Computer Security*, Vol. ahead-of-print No. ahead-of-print.
<https://doi.org/10.1108/ICS-01-2021-0002>
- Stewart, H. (2022), "A systematic framework to explore the determinants of information security policy development and outcomes", *Information and Computer Security*, Vol. ahead-of-print No. ahead-of-print. <https://doi.org/10.1108/ICS-06-2021-0076>
- Stewart, H. (2022), "Security versus Compliance: An Empirical Study of the Impact of Industry Standards Compliance on Application Security", *International Journal of Software Engineering and Knowledge Engineering*, Vol. 32. <https://doi.org/10.1142/S021819402250015>.
- Stewart, H. (2022) 'Digital Transformation Security Challenges, *Journal of Computer Information Systems*, DOI: 10.1080/08874417.2022.2115953
- Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., Hahn, A.: NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security Revision 2. Tech. rep., NIST (2015)
- Suárez-Barraza, M. F., & Lingham, T. (2008). Kaizen within Kaizen teams: continuous and process improvements in a Spanish municipality. *Asian Journal on Quality*, 9(1), 1-21.
- Sveen, F. O., Torres, J. M., and Sarriegi, J. M. 2009. "Blind Information Security Strategy," *International Journal of Critical Infrastructure Protection* (2:3), pp. 95-109.

- Tang, J., Wang, D., Ming, L., & Li, X. (2012). A Scalable Architecture for Classifying Network SecurityThreats. Science and Technology on Information System Security Laboratory.
- Tarazan, S, and Bostan, A. 2016. "Customizing SSL Certificate Extensions to Reduce False-Positive Certificate Error/Warning Messages," International Journal of Information Security Science (5:2), pp. 21-28
- Tashtoush, L. (2021), "The Role of Information Systems Capabilities in Enhancing the Organizational Performance", Journal of Information Systems and Informatics. 3. 303-328.
10.33557/journalisi.v3i2.129.
- Teece, D.J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. Strategic Management Journal, 28, 1319–1350.
- Teece, D.J. (2018). Dynamic capabilities as (workable) management systems theory. Journal of Management and Organisation, 24, 359–368.
- Terglav, K., Ruzzier, M.K. and Kaše, R. (2016), "Internal branding process: exploring the role of mediators in top management's leadership–commitment relationship", International Journal of Hospitality Management, Vol. 54 No. 1, pp. 1-11.
- Thorwat, S. R. (2018), "ICT in Higher Education: Opportunities of Urban Colleges and Challenges of Tribal Colleges", International Research Journal of Multidisciplinary Studies, 1-6.
- Toapanta, M., Nazareno, J., & Tingo, R. (2016). Analysis of the Appropriate Security Models to Apply in a Distributed Architecture. IOP Conference Series: Materials Science and Engineering. Guayaquil, Ecuador: IEEE.
- Tom Tervoort, Marcela Tuler De Oliveira, Wolter Pieters, Pieter Van Gelder, Silvia Delgado Olabarriga, Henk Marquering, "Solutions for Mitigating Cybersecurity Risks Caused by Legacy Software in Medical Devices: A Scoping Review", IEEE Access, vol.8, pp.84352-84361, 2020.
- Troyer, L. (2017), "Expanding sociotechnical systems theory through the trans-disciplinary lens of complexity theory", in Kahlen, J., Flumerfelt, S. and Alves, A. (Eds.), Transdisciplinary Perspectives on Complex Systems, Springer, Cham.

- Urbach, N., & Röglinger, M. (2018). Introduction to Digitalization Cases. How Organisations Rethink Their Business for the Digital Age. In N. Urbach & M. Röglinger (2018), Digitalization Cases. How organisationer Business for the Digital Age (pp. 1-14). Cham, Switzerland: Springer.
- Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, 28(2), 118-144.
- von Leipzig, T., Gamp, M., Manz, D., Schöttle, K., Ohlhausen, P., Oosthuizen, G., Palm, D., & von Leipzig, K., (2017). Initialising Customer-Orientated Digital Transformation in Enterprises. *Procedia Manufacturing* (8), 517-524.
- Wainwright M, Russell A. Using NVivo audio-coding: Practical, sensorial and epistemological considerations. *Soc Res Updat*. 2010. [December 9, 2014]. Available at: [google Scholar](#)
- Walsham, G. (2006), "Doing Interpretive Research," *European Journal of Information Systems* (15:3), pp. 320-330.
- Walsh M. Teaching Qualitative Analysis Using QSR NVivo. *Qual Rep*. 2003;8(2):251–256. [[Google Scholar](#)]
- Warner, K.S.R., & Wäger, M. (2019). Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal. *Long Range Planning*, 52, 326–349
- WEF, W. (2019), "The global risks report 2019", World Economic Forum Switzerland, Geneva.
- Wessel, L., Baiyere, A., Ologeanu-Taddei, R., Cha, J., & Jensen, T. B., (2020). Unpacking the Difference between Digital Transformation and IT-Enabled Organisational Transformation. *Journal of Association of Information Systems*, 22(1), 102-129
- Whitman, M., & Mattord, H. (2009), "Principles of information security (3rd ed.). Boston, MA: Course Technology.
- Williams, A. (1968), 'Interviewer role performance: A further note on bias in the informant interview', *Public Opinion Quarterly*, 32 (2), pp.287-94.
- Witmer, D. F. Colman, R. and Katzman, S. L.(1999), "From paper-and-pencil to screen-and-keyboard: Towards a methodology for survey research on the Internet, in Jones, S. (Ed.) *Doing Internet Research: Critical Issues and Methods for Examining the Net*. London. Sage. pp. 145-161.

Yahoo (2023) Data Leakage. Available from: shorturl.at/EMRY7 [accessed Jan 05 2023].

Yang, M.-X., Yuan, L.-N., & Yang, Z.-X. (2010). A discuss of computer security strategy models. International Conference on Machine Learning and Cybernetics (pp. 20-33). Qingdao, China: IEEE.

Yee, K. P. 2004. "Aligning Security and Usability," IEEE Security & Privacy (1:5), pp. 48-55.

Yeniman, Y., Ebru Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing information security management in small-and medium-sized enterprises: a case study from turkey. International Journal of Information Management, 31(4), 360–365.

Yin, R. (2014). Case Study Research: Design and Methods (5th ed.). Thousand Oaks, CA: Sage Publications, Inc.

Zhao, Y., & Lang, B., Liu, M., (2017), "Ontology-based unified model for heterogeneous threat intelligence integration and sharing", 11-15. 10.1109/ICASID.2017.8285734.

Zoto, E., Kowalski, S., Lopez-Rojas, E. A., & Kianpour, M. (2018), "Using a socio-technical systems approach to design and support systems thinking in cyber security education," 4th International Workshop on Socio-Technical Perspective in IS development (STPIS'18) (pp. 123-128). Tallinn]-Estonia: 4th International Workshop on Socio-Technical Perspective in IS development (STPIS'18).

Chapter 11.

Appendix

11.1 PAPER 1

11.1.1 Value Added Justification

DT brings undeniable value to businesses and organisations. It involves automating manual processes, streamlining workflows, and implementing advanced technologies to increase efficiency and productivity. By reducing the need for manual labour, digital transformation can lead to cost savings. This, in turn, allows businesses to cut operational costs, reduce overhead, and allocate resources to more strategic areas. Digital systems can be easily scaled to accommodate business growth, making it easier to seize new opportunities and adapt to changes in demand (Grazioli & Jarvenpaa, 2000).

Cloud-based systems and remote work capabilities can ensure business continuity. Enhancing the customer experience by providing personalisation, faster response times, and better accessibility is a primary focus of many digital transformation initiatives. Satisfied customers are likely to remain loyal and recommend a business to others (Datta, 2011).

DT enables organisations to collect and analyse vast amounts of data, which they can use to make informed decisions, identify trends, and respond to changing market conditions effectively.

Furthermore, it encourages organisations to adopt a culture of innovation and adaptability, allowing them to react quickly to market changes and stay competitive (Pikkarainen et al., 2004).

Successful implementation of DT gives companies a competitive edge, and they can offer new services, products, or business models that others may struggle to replicate. Global expansion is another value of DT by breaking down geographical barriers. Companies can reach and serve customers worldwide, opening up new revenue opportunities (Howcroft et al., 2002).

Modernising tools and processes can improve employee satisfaction and engagement by allowing them to focus on more strategic and creative tasks rather than repetitive, mundane work. Furthermore, DT can reduce the environmental impact of a business by minimising the use of paper, optimising energy consumption, and supporting remote work, which reduces commuting and office space requirements.

Adhering to regulatory requirements is critical for many industries. DT can help businesses maintain compliance and streamline reporting. With digital systems, organisations can track actions and transactions more efficiently, enhancing transparency and accountability within the company. Digital tools provide valuable insights into customer behaviour and market trends, which helps companies tailor their products and services to meet customer demands effectively (Howcroft et al., 2002).

In summary, DT brings significant value to businesses by improving operational efficiency, customer experience, innovation, and overall competitiveness. By allowing organisations to adapt to the changing business landscape, stay relevant, and thrive in the digital age.

11.1.2 Customer's Trust Justification

Maintaining customer trust is crucial for the success of any organisation's digital initiatives. Organisations often invest in robust cybersecurity solutions and practices to achieve this, demonstrating their commitment to protecting customer data. With regulations like GDPR (General Data Protection Regulation), organisations are compelled to respect and protect customer privacy. Transparency in business operations is essential for building trust and showing a commitment to accountability. Digital transformation initiatives often focus on increasing transparency and contributing to customer satisfaction by openly communicating intentions, processes, and data usage policies (Yao et al., 2003).

DT also enables businesses to provide better and more efficient customer support. Features like chatbots, self-service portals, and omnichannel communication make it easier for customers to get assistance when needed, leading to higher satisfaction and trust in the company. Personalization is a crucial aspect of digital transformation that allows businesses to offer customised experiences to their customers. This demonstrates an understanding of their customers' needs and preferences, which can enhance trust and customer loyalty (Luarn and Lin, 2005).

Furthermore, cloud-based solutions are often utilised in digital transformation, which can lead to improved reliability and availability of services. This consistency in delivering products or services without downtime or disruptions fosters trust in the brand and its commitment to meeting customers' needs (Modi et al., 2012; Coppolino et al., 2016; Ramachandran, 2015).

DT also makes it easier for customers to access and interact with businesses. Collecting customer feedback and using it for continuous improvement is crucial for any business. When customers see that their feedback is taken seriously, it builds trust and shows a commitment to meeting their needs. The

convenience of online shopping, digital banking, and other digital services fosters trust in the brand and its commitment to meeting customers where they are. Businesses that embrace DT are better positioned to adapt to changing customer preferences and market trends. This adaptability and willingness to innovate demonstrate a long-term commitment to customers, which builds trust (Sari, 2015).

In summary, by prioritising security, privacy, transparency, and customer-centric practices, organisations can maintain customer trust, which is essential for long-term success in the digital era.

11.1.3 Data Security Justification

A crucial element of digital transformation is ensuring data security, which is essential for the success and sustainability of any digital initiative.

Data security is paramount in digital transformation as it helps protect sensitive customer, employee, and proprietary data. This includes personal information, financial data, intellectual property, and trade secrets. Organisations need to ensure they safeguard this data, not only to demonstrate their commitment to protecting the privacy and interests of stakeholders but also to comply with strict data protection regulations such as GDPR and HIPAA. Compliance with these regulations is mandatory, and non-compliance can result in severe legal and financial consequences. By implementing robust data security measures, organisations can justify their adherence to these regulations (Armbrust et al., 2010; Suthaharan & Panchagnula, 2012; Sari, 2015).

Data breaches and security incidents can severely damage an organisation's reputation and erode trust among customers and partners. Prioritising data security is a way for organisations to demonstrate their dedication to maintaining trust and protecting the integrity of their brand. Data breaches can be costly, with expenses related to detection, response, notification, legal action, and potential fines. Managers who invest in data security measures can help mitigate these financial risks and justify the associated costs (Al-shqeerat et al., 2017; Djemame, 2016; Nada et al., 2017; Rot, 2017; Wang, 2017).

Organisations with a solid commitment to data security often have a competitive edge since they can assure customers and partners that their data is safe, making them more attractive in the market. Additionally, many businesses rely on intellectual property as a critical asset. Data security measures protect proprietary information, trade secrets, and innovations, ensuring they remain confidential and valuable (Kozlov et al., 2018; Esposito & Castiglione, 2017).

Data security is crucial in digital transformation because data is a valuable resource for making informed decisions and gaining insights into customer behaviour and market trends. Ensuring the security of this data is crucial to justify investments in analytics and data-driven decision-making. In a digital ecosystem, where organisations often share data with vendors, partners, and third-party service providers, strong data security practices help build trust among these entities and justify collaboration (Mostajeran et al., 2017; Belbergui, 2017; Lee, 2012; Al-shqeerat et al., 2017).

In summary, data security is essential in digital transformation to protect sensitive information, comply with regulations, maintain trust, mitigate financial risks, and gain a competitive advantage. It is a crucial aspect of a successful and sustainable digital transformation strategy, ensuring that organisations can thrive in the digital age while protecting their stakeholders' interests.

11.1.4 User Interface Design (UI) Justification

The significance of user interface (UI) design in digital transformation is underscored by several factors. These include improving the user experience, optimising efficiency, and achieving the goals of digital initiatives (Clark, 2002).

Digital transformation aims to improve the user experience. A well-designed user interface (UI) places the user at the centre of the transformation process, ensuring that digital tools and systems are intuitive, user-friendly, and responsive to user needs. A visually appealing and intuitive UI design creates a positive and engaging experience for users, enhances satisfaction, reduces friction in interactions, and can lead to increased customer loyalty and retention (Clark, 2002; Al-Matari et al., 2020).

A well-designed UI streamlines processes, reduces the learning curve for new digital tools, and simplifies complex tasks. This efficiency not only benefits users but also leads to time and cost savings for the organisation. A consistent and well-designed UI maintains a sense of familiarity for users across different digital channels, applications, and devices. This consistency helps users feel more comfortable and confident while interacting with the organisation's digital assets (Duc & Chirumamilla, 2019; Ande et al., 2020).

A thoughtfully designed UI considers the diverse needs of users, including those with disabilities. By ensuring accessibility and inclusivity, organisations can reach a broader audience and demonstrate a commitment to social responsibility. Other factors, such as brand identity and trust, competitive advantage in the digital age, and user experience, are key differentiators. A well-designed UI can

provide a competitive advantage by attracting and retaining customers who value superior digital interaction. A visually appealing and user-friendly UI can encourage users to engage more with digital products or services, increasing their time on the platform and leading to higher conversion rates and user engagement (Duc & Chirumamilla, 2019).

UI can also enhance managers' data-driven decision-making since UI design can incorporate analytics and user behaviour data to inform iterative improvements. Furthermore, scalability and ease of integration simplify adding or updating features as part of the digital transformation (Duc & Chirumamilla, 2019).

In summary, UI design is a critical component of digital transformation because it directly impacts user satisfaction, efficiency, and achieving transformation goals. A well-designed UI not only enhances the user experience but also provides tangible business benefits, such as increased customer loyalty, cost savings, and a competitive edge in the digital landscape.

11.1.5 FinTech Promotion Justification

DT has numerous benefits for individuals, businesses, and the economy. With FinTech, underserved or unbanked populations gain access to financial services. By using mobile and digital technologies, people with limited access to banking services can manage their finances, save money, and participate in the formal economy. This reduces the costs of traditional financial services, resulting in lower fees, better interest rates, and more affordable financial products (Ahluwalia et al., 2020).

FinTech services are usually available 24/7, providing users convenient access to their financial accounts, transactions, and services through web and mobile applications. This accessibility is essential in today's fast-paced world, as it promotes faster payment processing and fund transfers. Businesses can streamline their operations, and consumers can expect quick and convenient financial transactions (Ahluwalia et al., 2020).

FinTech companies invest in user interface and user experience design, making their platforms easy to navigate and user-friendly. This enhances the customer experience, leading to increased adoption and customer loyalty. This innovation fosters further innovation in the financial industry, promoting new technologies such as blockchain and artificial intelligence that are being used to create novel financial products and services, from cryptocurrency to robo-advisors. These innovations provide users with more choices and better financial solutions (Nakashima, 2018).

FinTech solutions cater to small and medium-sized enterprises (SMEs), offering tools for managing finances, accessing capital, and streamlining payment processes. This can fuel economic growth by empowering small businesses. FinTech companies leverage data analytics to make more informed financial decisions, benefiting individuals and businesses by helping them manage their finances more effectively. FinTech systems are designed to be resilient, providing financial services even in adverse conditions, such as natural disasters or disruptions. This ensures business continuity and access to financial assistance when needed (Zavolokina, et al., 2016; Anagnostopoulos, 2018).

In summary, promoting FinTech is justified due to its potential to enhance financial inclusion, reduce costs, improve convenience, drive innovation, increase transparency, and foster economic growth. By embracing FinTech, individuals and businesses can access various benefits contributing to improved financial well-being and overall economic development.

11.2 Basis of Assumption

DT introduces several security challenges that can lead to unpredictable outcomes. It is challenging to make specific predictions about these uncertainties (Collett, 2020; Karpunina et al., 2019).

The cybersecurity landscape constantly evolves, and new threats and vulnerabilities emerge regularly. Even if organisations invest in security measures, they may still be vulnerable to unknown or zero-day attacks. Therefore, it is uncertain whether all security challenges can be entirely addressed (Andriotis et al., 2015; DeWitt et al. (2015).

Human behaviour and awareness within organisations can unintentionally or intentionally compromise security. The efficacy of security solutions in mitigating these challenges can be uncertain because it depends on human factors (Mlitz, 2021; Duc & Chirumamilla, 2019).

Furthermore, DT often involves complicated IT systems and interconnected networks. The interaction of different technologies and the possibility of unforeseen interactions make it difficult to predict all possible security challenges and their consequences. This is particularly true for enterprises that rely on third-party vendors and service providers as part of their DT efforts. These third-party providers may introduce new risks, and the ability to control and predict their security outcomes may be limited (Li et al., 2020; Karpunina et al., 2019).

In addition, external factors such as privacy and security regulations may change over time. Companies may need to adapt their security measures to comply with new rules, which can create uncertainty in their security posture (Eamon et al., 2013). Other factors, such as limited resources, emerging technologies, economic change, economic conditions, cultural factors, and geopolitical considerations, can be uncertain and challenging (O'Reilly, 2013).

In summary, addressing security challenges during digital transformation can be uncertain due to the dynamic and ever-changing nature of the cybersecurity landscape, the complexity of digital systems, and the impact of various external and internal factors. While organisations may implement security measures and strategies, outcomes are not always predictable, and constant vigilance and adaptability are essential to address new threats and challenges.

11.3 PAPER 2

11.3.1 Banks in Germany's intention to adopt IaaS are not always influenced by the organisational factor (Justification)

The decision to adopt Infrastructure as a Service (IaaS) in an organisation is not solely influenced by organisational factors. Technical, economic, and cultural aspects can also be important in the decision-making process.

Technical requirements can vary significantly between organisations. Some organisations may find IaaS the best fit based on their technical needs, while others may find alternative solutions more suitable. For example, an organisation heavily relying on internal data centres may choose a different approach, even if the corporate culture or structure suggests otherwise. Additionally, the cost of IaaS adoption can be a significant factor. For some enterprises, IaaS may be cost-effective. In contrast, for others it may not be based on budget constraints, existing infrastructure investments, and the cost of migrating to cloud-based solutions (Ahluwalia et al., 2020).

Economic factors also often play a central role in the decision-making process. Other factors, such as significant investment in local Infrastructure, risk tolerance, corporate culture, and regulatory and compliance factors, sometimes outweigh other organisational factors. In addition, the size and scope of an organisation, corporate strategies and long-term goals, and existing relationships with technology vendors and service providers can also influence the adoption of IaaS (Nakashima, 2018).

11.3.2 Consumer trust does not always influence organisations' intention to adopt cloud platforms (IaaS) (Justification)

Consumer trust is a crucial factor for many organisations, but it may not always be the sole determinant of their intention to adopt Infrastructure as a Service (IaaS) cloud platforms. There are various reasons why consumer trust may not have a direct influence on IaaS adoption. For instance, many cloud platforms primarily target business-to-business (B2B) markets, where cost savings, scalability, and technical capabilities are prioritised over consumer trust (Duc & Chirumamilla, 2019).

Additionally, the decision-making process for IaaS adoption is complex and involves various stakeholders, such as IT departments, procurement teams, and top management. These stakeholders consider technical, financial, and operational aspects alongside consumer trust. Organisations may prioritise their data security and compliance requirements over consumer trust and the need to ensure that IaaS providers can meet industry-specific security standards and regulatory compliance (Ande et al., 2020).

Furthermore, economic considerations such as cost-effectiveness and return on investment (ROI) are significant drivers for IaaS adoption. Even if consumer trust is high, organisations may choose IaaS based on economic and technical performance factors rather than trust alone. Technical performance, including uptime, reliability, and network speed, is crucial in IaaS adoption. Organisations may also prioritise these factors when evaluating cloud providers (Duc & Chirumamilla, 2019).

While consumer trust in cloud providers is essential, organisations may also assess the reputation and track record of cloud vendors from a business perspective, focusing on reliability, support, and service level agreements. Depending on the organisational goals, such as digital transformation initiatives, these strategic objectives may take precedence over consumer trust (Carlson, 2015).

Adopting IaaS cloud platforms is influenced by a broad spectrum of factors, which may sometimes outweigh or override consumer trust considerations. Decisions related to IaaS adoption are complex and multifaceted and may vary from organisation to organisation. Although consumer trust is essential for specific organisations, it may not always be the determining factor in IaaS adoption conditions offered by providers (Straub et al., 1997).

11.3.3 The willingness of banks in Germany to trust IaaS is not influenced by data security (Justification)

It is not possible to support this hypothesis because data security is a significant factor that affects whether banks in Germany are willing to trust Infrastructure as a Service (IaaS). The financial sectors must comply with strict regulatory standards related to data protection and privacy, such as the General Data Protection Regulation (GDPR). Data security is a crucial aspect of compliance, and banks must ensure that their data is secure, whether stored on-premises or in the cloud (Carlson, 2015).

Banks rely on their customers' trust, and any data security breach can have severe consequences, including damage to the bank's reputation and loss of customer trust. Therefore, banks must ensure that sensitive data is protected and confidentiality is maintained when using IaaS platforms. The financial sector is vulnerable to various cyber threats, including hacking, data breaches, and fraud. As a result, confidentiality is of utmost importance for banks (Straub et al., 1997).

Data encryption is a critical factor that IaaS providers typically offer both in transit and at rest. Encryption is a fundamental component of data security, and banks must protect their data against unauthorised access. In addition to encryption, Identity and Access Management (IAM), Security Audits and Compliance, Incident Response and Disaster Recovery, Data Residency and Sovereignty are necessary concerns that IaaS providers must offer at all their data centres in all geographic regions (Sharma & Trivedi, 2014).

In conclusion, data security plays a central role in determining the trust of banks in Germany towards IaaS. While IaaS can provide many benefits, banks must ensure that their data is secure and compliant with regulatory standards and that customer trust is maintained. Reputable IaaS providers invest heavily in security measures, making them a reliable choice for banks looking to benefit from cloud services while maintaining data security (Al-Khater, et al., 2020).

11.3.4 Data security does not influence banks in Germany's intention to adopt IaaS (Justification)

The hypothesis that banks in Germany are open to the introduction of Infrastructure as a Service (IaaS) without considering data security is not tenable. Banks worldwide, including in Germany, place great

emphasis on data security when introducing any technology, including IaaS. Therefore, it would be dubious for banks to disregard data security concerns when introducing IaaS (Al-Khater et al., 2020).

The banking sector is subject to strict data protection and privacy regulations in many countries due to various factors, such as strict regulatory and legal requirements. Banks must ensure adequate protection for customer data, financial information, and other sensitive data to avoid legal consequences, fines, and reputational damage (Belbergui, 2017).

Trust and customer confidence are paramount since data breaches or security lapses can erode trust, leading to customer attrition and reputational damage. The Cyber Threat Landscape has become sophisticated, and the banking industry is a prime target for cyberattacks, including ransomware, phishing, and data breaches, which are on the rise. In addition, banks must ensure that they treat customer data with the utmost confidentiality and care, as data privacy is a significant concern.

To maintain operational resilience, banks must implement data encryption, incident response and recovery, vendor due diligence, audit, and well-established risk management practices as part of their cybersecurity framework. The adoption of IaaS is subject to rigorous risk assessments (Babak et al., 2015).

Ensuring data security is an essential and non-negotiable requirement for banks in Germany when it comes to adopting IaaS. IaaS providers must meet the strict data security standards and requirements to be considered feasible. In summary, data security is a crucial aspect that cannot be compromised.

11.3.5 Banks in Germany' intention to adopt IaaS is not influenced by the technological factor (Justification)

Several factors influence the adoption of Infrastructure as a Service (IaaS) in the banking industry beyond technological considerations. Although technology is crucial to adopting IaaS, other factors are equally important, such as the heavily regulated nature of the banking industry. Banks must adhere to strict requirements for data security, privacy, and compliance. Therefore, any IaaS solution they adopt must comply with these regulations. The ability of IaaS providers to meet regulatory and compliance requirements is critical. Banks must also evaluate the security measures of IaaS providers, including data encryption, access controls, and incident response capabilities, since they are the custodians of sensitive customer and financial data (Babak et al., 2015).

There are other factors to consider, such as data residency and sovereignty, where banks must ensure that customer data is stored within a specific geographic location or under the jurisdiction of a particular country. Operational resilience service level agreements (SLAs) also play a significant role in IaaS adoption. Banks rely on SLAs to define the expected service quality, including uptime guarantees, response times, and support. Additionally, SLAs include contractual commitments related to performance, availability, and support. Other critical factors, such as IaaS provider reputation, Economic Factors, organisation Strategic Objectives, and Competitive Landscape, must be considered since banks have complex IT infrastructures and unique technology stacks. The ability to customise and integrate IaaS solutions with existing systems and applications is a significant consideration (Coppolino et al., 2016).

In summary, the decision to adopt IaaS by banks is influenced by many factors, including regulatory compliance, data security, operational resilience, contractual commitments, economic factors, strategic objectives, and organisational dynamics. It is essential to assess IaaS solutions holistically, given the highly regulated and complex nature of the banking industry.

11.3.6 Technological factors do not influence the willingness of banks in Germany to adopt IaaS (Justification)

It is improbable that banks in Germany would not be influenced by technological factors when considering the adoption of Infrastructure as a Service (IaaS). Technological factors are a critical consideration for any organisation, particularly in cloud adoption (Straub et al., 1997).

Banks have unique technological requirements that need to be met by IaaS solutions. One of the most critical factors is scalability, which allows banks to adjust their IT infrastructure according to their changing needs, workloads, and customer demands (Ahluwalia et al., 2020). The performance of IaaS solutions, such as processing power, speed, and network capabilities, is critical to ensure that banking operations run smoothly and efficiently. Additionally, high levels of system reliability and availability are essential to gain customers' trust (Stewart & Jürjens, 2018). Other important factors include the ability to store and manage large amounts of data securely and efficiently, with features such as encryption, access controls, and threat detection (Duc & Chirumamilla, 2019; Ande et al., 2020). The compatibility of IaaS solutions with the bank's existing IT infrastructure is also a significant consideration.

Furthermore, IaaS solutions that can transfer large volumes of data quickly and securely offer technological capabilities for disaster recovery and data backup for business continuity, virtualization, orchestration, optimising resource utilisation, reducing infrastructure costs, and providing innovative technologies such as artificial intelligence, machine learning, and advanced analytics can give banks a competitive edge. These factors significantly impact their decision to adopt IaaS solutions (Duc & Chirumamilla, 2019; Ande et al., 2020).

In summary, the adoption of IaaS by banks in Germany hinges on several crucial technological factors. The technical capabilities, performance, and compatibility of IaaS solutions play a critical role in supporting their operations, ensuring security and compliance, and driving innovation. It is not easy to imagine that technological factors do not have a significant impact on banks' willingness to adopt IaaS.

11.3. 7 Environmental factors are not a vital determinant of consumer trust in banks' intention to adopt IaaS (Justification)

Environmental factors may not directly determine consumer trust in banks' intention to adopt Infrastructure as a Service (IaaS) in the context of ecological or environmental sustainability. Although environmental factors are essential for banks and other organisations regarding corporate responsibility and sustainability, they may not hold the same weightage in consumer trust or IaaS adoption (Straub et al., 1997).

Various factors influence consumer trust in banks. Among them, data security, privacy, financial stability, and the bank's ability to protect and manage their money are the most important. These factors have a direct and immediate impact on consumer trust. Regulatory bodies and authorities govern the banking industry, setting standards and requirements for financial services, data security, and consumer protection. While some regulations may touch on sustainability and environmental responsibility, they are usually not the primary focus (Duc & Chirumamilla, 2019; Ande et al., 2020).

Although banks may have sustainability and environmental responsibility efforts in place, they are not the primary factors that drive consumer trust. Consumers are more concerned about the security and privacy of their personal and financial information, the financial stability of banks and their ability to protect and grow their investments. These factors are more closely tied to the core banking functions and are thus more important than sustainability efforts. Investment decisions, marketing, brand image, and cultural and regional variations are all complementary efforts to the core business, but they are not the primary drivers of consumer trust (Duc & Chirumamilla, 2019; Ande et al., 2020).

In conclusion, environmental factors, while playing a critical role in corporate responsibility and sustainability, are not the primary factors determining consumer trust in banks' intentions to adopt IaaS or in the banking sector as a whole. Consumer trust in banking is more directly influenced by data security, privacy, financial stability and the overall quality of banking services at the centre of the banking sector.

11.4 PAPER 4

Table 4. Factors affecting the security of the information system or digital transformation

DSS Constructs		Definition	References
Security Misperception	SM	IS/IT Strategy and Digital Strategy Misconception	(Collett, 2020) Karpunina et al. (2019) (Andriotis et al. (2015) DeWitt et al. (2015) (Dhillon et al. (2016). Mlitz (2021) Duc & Chirumamilla (2019) Li et al. (2020) Karpunina et al. (2019) Eamon et al. (2013) O'Reilly (2013)
Evaluation of threat Vulnerability and Risk	ETVR	Threats, vulnerabilities, and mitigation techniques that are linked to the digital strategy and assist to reduce the overall risk.	Collett (2020) Yan et al. (2013) Yu et al. (2006) Cuchta (2019) Chooi & Ahmad (2017) Hussain (2018) Lucila (2016) Flowerday & Tuyikeze (2016) Sohrabi et al. (2016) Joshi et al. (2017)

			Karumbaiah et al. (2016)
Cybersecurity Strategy	CSS	Action plan to improve the security and resilience of electronic products and services. It is an overarching, top-down strategy for cybersecurity that sets out a series of goals and priorities to be achieved within a specific timeframe.	Collett (2020) Stewart (2021) Chooi & Ahmad (2017). Lucila (2016) Flowerday & Tuyikeze (2016) Sohrabi et al. (2016) Joshi et al. (2017) Karumbaiah et al. (2016)
Secure System Engineering	SSE	Integration of secure software engineering tools, methodologies, and processes into the software life cycle.	Mlitz (2021) Collett (2020) Duc & Chirumamilla (2019) Doukidis et al. (2020)
Security Testing and Evaluation	ST&E	Analyse and assess the security measures required to secure digital services and goods. Reduces threats and risks in systems and lowers the likelihood of losses due to a cybersecurity breach.	Bertolino et al. (2014) Ayewah et al. (2008) Acker et al. (2012) Appelt et al. (2014)
Protective Monitoring	PM	Automatic security checks based on logs created by systems or applications.	Moeini et al. (2019) Da Veiga & Martins (2015) Luo et al. (2019) Terglav et al. (2016) Collett (2020)
Strategic Advanced Threat Intelligence	SATI	Strategic threat intelligence provides a comprehensive Overview of an organisation's threat landscape.	Padayachee (2012) Stewart (2022) Piplai et al. (2020) Puyt et al. (2020) Sahrom et al. (2018). Tounsi & Rais (2018) Verizon (2020)

Incident Response and Remediation	IRR	Respond to incidents quickly and efficiently to maximise effectiveness.	<p>WEF (2019)</p> <p>Morgeson et al. (1997)</p> <p>Ahmad et al. (2012)</p> <p>Helsloot & Groenendaal (2011)</p> <p>Ahmad et al. (2021)</p>
-----------------------------------	-----	---	--

11.5 References:

I. Anagnostopoulos, Fintech and Regtech: impact on regulators and banks, *J. Econ. Bus.* 100 (11–12) (2018) 7–25

Cuchta, T.; Blackwood, B.; Devine, T.R.; Niichel, R.J.; Daniels, K.M.; Lutjens, C.H.; Maibach, S.; Stephenson, R.J. (2019), “Human Risk Factors in Cybersecurity. In Proceedings of the 20th Annual SIG Conference on Information Technology Education, Tacoma, WA, USA, 3–5 October 2019; pp. 87–92

Hussain, H.S.; Din, R.; Khidzir, N.Z.; Daud, K.A.M.; Ahmad, S. (2018) Risk and Threat via Online Social Network among Academia at Higher Education. *J. Physics: Conf. Ser.* 2018, 1018, 012008

L. Zavolokina, M. Dolata, G. Schwabe, The FinTech phenomenon: antecedents of financial innovation perceived by the popular press, *Finan. Innov.* 2 (2016) 1–16.

Piplai, A., Mittal, S., Abdelsalam, M., Gupta, M., Joshi, A., & Finin, T. (2020). Knowledge Enrichment by Fusing Representations for Malware Threat Intelligence and Behavior. 2020 IEEE International Conference on Intelligence and Security Informatics (ISI).
<https://doi.org/10.1109/isi49825.2020.9280512>

Puyt, R., Lie, F. B., De Graaf, F. J., & Wilderom, C. P. M. (2020). Origins of SWOT Analysis. *Academy of Management Proceedings*, 2020(1), 17416. <https://doi.org/10.5465/ambpp.2020.132>

S. Ahluwalia, R.V. Mahto, M. Guerrero, Blockchain technology and startup financing : a transaction cost economics perspective, *Technol. Forecast. Soc. Change* 151 (2020) 119854.

Sahrom Abu, M., Rahayu Selamat, S., Ariffin, A., & Yusof, R. (2018). Cyber Threat Intelligence – Issue and Challenges. *Indonesian Journal of Electrical Engineering and Computer Science*, 10(1), 371. <https://doi.org/10.11591/ijeecs.v10.i1.pp371-379>

T. Nakashima, Creating credit by making use of mobility with FinTech and IoT, *IATSS Res.* 42 (2) (2018) 61–66.

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, 72, 212–233. <https://doi.org/10.1016/j.cose.2017.09.001>

Verizon, D. (2020). Data Breach Investigations Report 2020. *Computer Fraud & Security*, 2020(6), 4. [https://doi.org/10.1016/s1361-3723\(20\)30059-2](https://doi.org/10.1016/s1361-3723(20)30059-2)

Yan J, Govindarasu M, Liu C-C, Vaidya U. A (2013), PMU-based risk assessment framework for power control systems. In: *Power and energy society general meeting (PES)*. IEEE; 2013. p. 1–5.

Yu J, Mao A, Guo Z. (2006), “Vulnerability assessment of cyber security in power industry”, In: *Power systems conference and exposition (PSCE)*. IEEE; 2006. p. 2200–5.