Flinders University

Enhancing IoT Cybersecurity Frameworks

By

Scott William Anderson

Bsc(CyberSecurity), Bsc(Security)Hons

Thesis Submitted to Flinders University for the Degree **Doctor of Philosophy (PhD)**

College of Science and Engineering

1st November 2023

DECLARATION

I certify that this thesis:

1.) Does not incorporate without acknowledgment, any material previously submitted for a degree or diploma in any university; and
2.) and the research within will not be submitted for any other future degree or diploma without the permission of Flinders University; and
3.) To the best of my knowledge and belief, does not contain any material previously published or written by another person except where due reference is made in the text.

____*Signature Redacted*____

Scott William Anderson

1st November 2023

ACKNOWLEDGEMENTS

I would like to acknowledge my wonderful wife (who, when I first started this journey, was titled as girlfriend!) Sarah, who without her tireless support, understanding, and assistance this PhD journey would have never started. To my mentor and primary supervisor Trish Williams, for always being there when needed, even when the hours were quite strange, and to Vincent McCauley, who's different views gave me the perspective needed at critical junctions. To the new friends and family that I have gained along the way – thank you for the distractions, as strange as that sounds! Finally, a thanks to the Australian Government Research Training Program Scholarship 'Fee Offset' scheme, and I should also note the distinct lack of any professional editorial services in the creation of this thesis.

PUBLICATION LIST

Anderson, S., & Williams, T. (2017). Cybersecurity and Medical Devices: Are the ISO/IEC 80001-2-2 Technical Controls up to the Challenge? *Computer Standards & Interfaces*. (Anderson & Williams, 2017)

Honan, R., Lewis, T. W., Anderson, S., & Cooke, J. (2020). A Quantum Computer Operating System. In M. Qiu (Ed.), *Algorithms and Architectures for Parallel Processing* (pp. 415–431). Springer International Publishing.(Honan et al., 2020)

ABSTRACT

BACKGROUND

The term Internet of Things (IoT) was coined in 1999. Though the term has been around for nearly two decades, IoT does not yet possess an accepted, singular definition. This lack of cohesion hampers the critical aspect of cybersecurity for IT systems involving IoT, as cybersecurity relies on clear and defined systems and boundaries. When lacking these clear boundaries, the subsequent nonstandard approaches to cybersecurity performed to address the lack of boundaries and the rise in popularity of IoT present a critical issue. As IoT devices become more popular, their application in healthcare ranges from clinical usage in hospitals to personal monitoring devices used for everyday health monitoring.

PROBLEM

The need for effective cybersecurity is compounded with the rapid application across multiple areas, from healthcare to industrial. The usage of IoT across such diverse settings has led to new applications of IoT technology, creating a multitude of new terms. This adaptation of physical interactions in many new areas of application has as added urgency to the requirement for appropriately reliable cybersecurity in healthcare. Currently, there is a lack of clear guidance for IoT Cybersecurity.

METHODOLOGY

This research analysed the current state of the IoT, analysing existing definitions and system boundaries; these system boundaries informed the creation of a framework for applying cybersecurity to IoT Devices. To complete this research, a multi-stage project governed by the theory of information systems, and multiple Case Studies was undertaken. Utilising multiple Case Studies to create analysis boundaries allowed for both individualistic analysis of the components of IoT systems and a holistic view of the systems that include IoT.

FINDINGS

The resulting framework addresses the deficiencies in IoT Cybersecurity by identification of IoT specific actions in comparison to contemporary best practice for cybersecurity, resulting in a

framework that fills the gaps in current IoT cybersecurity guidance. This framework is applicable to all deployments of IoT.

IMPACT

By clearly identifying the deficient aspects of current guidance and tailoring solutions to the unique limitations of IoT, all interested parties of IoT devices gain a greater understanding of the overall cybersecurity posture of their application of IoT. The approach of creating a cybersecurity framework as an overlay forms the basis for an entirely new way to think about the creation of cyber protective guidelines and frameworks – creating safer and more secure IoT networks. This results in greater coherence of the cybersecurity guidance for IoT, which will enhancing the effectiveness of guidance within IoT cybersecurity, ultimately enhancing the overall cybersecurity of the IoT ecosystem.

Table of Contents

1 Introduction..15
1.1 The Current State of The Internet of Things..16
1.2 The Healthcare Internet of Things and the associated problem..17
2 Literature Review..19
2.1 Terminology Challenges..20
2.2 IoT Perspectives..23
2.2.1 HIoT..26
2.3 IoT Technologies..26
2.3.1 Infrastructure..26
2.3.2 Platforms..29
2.3.3 Devices..31
2.3.4 Protocols..32
2.4 IoT Usage..34
2.4.1 History..34
2.4.2 Marketing and Consumer Expectations..37
2.4.3 Adoption..41
2.4.4 Ethics and Data Protection Legislation..42
2.5 IoT Cybersecurity..44
2.5.1 Problematic Concepts in IoT Cybersecurity..45
2.5.2 Shortfall in IoT Security Frameworks..48
2.6 Problems in IoT..52
2.6.1 Issues in HIoT..53
2.6.2 Issues with Terminology..54
2.6.3 Alternative Approaches..55
2.6.4 Ecosystem Wide Issues..56
2.7 Literature Summary..57
3 Methodology..58
3.1 Conceptual Frameworks..59
3.1.1 Positioning Theory..62
3.1.2 Managing Research Interpretation..63
3.1.3 Reason..64
3.1.4 Rigour..64

3.2 Methods 65
3.2.1 Research Questions 65
3.2.2 Selected Method 69
3.3 Research Design....75
3.3.1 Selection of Cases 76
3.3.2 Reason in Case Studies....76
3.3.3 Rigour in Case Studies 77
3.3.4 Case Study Layout....82
3.3.5 Design of Cross Analysis of Cases 82
3.3.6 Multiple Case Study Design 83
3.3.7 Detailed Case Design 85
4 Case 1: IoT Networks and Systems 99
4.1 Contextual Notes 99
4.2 Case Specific Inputs 99
4.3 Intended Case Outputs....99
4.4 Case Location in the Research Design....100
4.5 Case Content 100
4.5.1 Terminology....102
4.5.2 Language and Context 102
4.5.3 Categorising IoT....118
4.6 Conclusions 119
4.7 Issues Encountered During Case....120
4.8 Changes to Research Views....120
4.9 Learning from Case....121
5 Case 2-A: Cybersecurity & Network Technical Controls 122
5.1 Contextual Notes 123
5.1.1 Case-Specific Notes....123
5.2 Case Specific Inputs 123
5.3 Intended Case Outputs....123
5.4 Case Location in the Research Design....124
5.5 Case Content 124
5.5.1 Why Current Practice Fails....124
5.5.2 NIST Baseline Document Overview....124

5.5.3 Overview of Selected IoT Cybersecurity Documents ... 126
5.5.4 Target Audiences ... 128
5.5.5 Document Goals ... 129
5.5.6 Document to Capability Mapping ... 136
5.5.7 Capability Explanation ... 138
5.5.8 Document Overview: AGELIGHT ... 140
5.5.9 Document Overview: BITAG ... 147
5.5.10 Document Overview: CSA ... 154
5.5.11 Document Overview: CSDE ... 159
5.5.12 Document Overview: CTIA ... 166
5.5.13 Document Overview: ENISA ... 171
5.5.14 Document Overview: ETSI ... 179
5.5.15 Document Overview: GSMA ... 184
5.5.16 Document Overview: IEC ... 193
5.5.17 Document Overview: IIC ... 200
5.5.18 Document Overview: IoTSF ... 211
5.5.19 Document Overview: OTA ... 219
5.5.20 Document Overview: NEMA ... 224
5.5.21 Document Overview: OCF ... 228
5.5.22 Document Overview: PSA ... 235
5.6 Conclusions ... 242
5.6.1 Overall Insights ... 242
5.6.2 Characteristic Summary ... 243
5.6.3 Additional Findings ... 249
5.7 Issues Encountered During Case ... 254
5.8 Changes To Researchers’ Views ... 255
5.9 Learning From Case ... 256
5.9.1 Level 1 learning ... 256
5.9.2 Level 2 learning ... 256
6 Analysis ... 257
6.1 Ecosystem Wide IoT Attributes ... 259
6.1.1 Cyber-Physical Systems (CPS) ... 259
6.1.2 Organisational Maturity ... 259

6.1.3 Modern Cryptography 260

6.1.4 Secure Data Storage and Transmission 260

6.1.5 Endpoint Management 262

6.1.6 Cybersecurity Policies 262

6.1.7 Device Reset and Refresh 262

6.1.8 Strong Defaults 263

6.1.9 Secure Provisioning and Updates 263

6.1.10 No Usage of Deprecated Protocols 264

6.1.11 Event Logging and Auditing 264

6.1.12 Hardware Secure Storage 264

6.1.13 Authentication and Authorization 265

6.2 NIST Traditional Cybersecurity Functions 266

6.2.1 Function: Identify 267

6.2.2 Function: Protect 273

6.2.3 Function: Detect 279

6.2.4 Function: Respond 283

6.2.5 Function: Recovery 286

6.3 Summary 288

7 Discussion 289

7.1 Unique IoT Considerations 292

7.1.1 Modern Cryptography 292

7.1.2 Secure Data Storage and Transmission 293

7.1.3 Strong Defaults 294

7.1.4 Secure Provisioning 295

7.1.5 Hardware Secure Storage 295

7.1.6 Authentication and Authorization 295

7.1.7 Tangential Security 297

7.1.8 Resilience by Design 297

7.1.9 Maintenance 297

7.2 Process Considerations 298

7.2.1 Asset Management 298

7.2.2 Disaster Recovery Planning 300

7.2.3 Policy Creation and Maintenance 300

7.3 How IoTSOF and IoTSOF-E Fill the Gap 302
7.4 Worked Example 306
7.4.1 Step One: Start 307
7.4.2 Step Two: Assess Framework Requirements 308
7.4.3 Step Three: Assess IoT Device Limitations 309
7.4.4 Step 4: Acceptable Level of Protection 311
7.4.5 Step Five: Resolve IoT Device Capabilities vs. Framework Requirements Conflicts 311
7.4.6 Step 6: Alter Device 312
7.4.7 Step 7: Return to Assess IoT Device Limitations 312
7.4.8 Step 8: Re-Assessment of Adequate Protection 313
7.4.9 Step 9: Implement Cybersecurity Protections 314
8 Conclusion 316
8.1 Answering the Question 316
8.2 Significance 317
8.2.1 Generalising the Research 317
8.2.2 The Overlay Approach 318
8.2.3 Common Basis 318
8.2.4 Language 319
8.2.5 Significance of the IOTSOF/E Framework 319
8.3 Conceptual Significance of the Research 320
8.3.1 Contribution to Knowledge 320
8.3.2 Contribution to Scholarship 320
8.3.3 Contribution to Practice 321
8.4 Personal Learnings 321
8.5 Future Research 322
8.6 Concluding Remarks 322
9 References 323
10 Appendix A: IoTSOF 346
11 Appendix B: IoTSOF-E 349

Table of Tables

Table 1: IoT Key Events Timeline 34
Table 2: Summary of Issues Identified form the Literature 56
Table 3: Research Methodology Overview, Adapted From (Anderson & Williams, 2017) 65
Table 4: Research Methodology Inclusion / Exclusion 66
Table 5: Research Methods Overview, Adapted From (Anderson & Williams, 2017) 66
Table 6: Research Method Inclusion / Exclusion 67
Table 7: Case Study Layout 82
Table 8: Case 2, Cybersecurity Principles Analysis Short Codes 92
Table 9: Case 2, Internal Cross Analysis Overview 93
Table 10: Case 4, Consumers Analysis Short-Codes 96
Table 11: Case 5, Enterprises Analysis Short-Codes 96
Table 12: Case 2 to Case 4, Cross-Analysis Overview 96
Table 13: Case 2 and Five, Cross-Analysis Overview 97
Table 14: Overall Case to Case Analysis Overview 98
Table 15: Major IoT Terminology 110
Table 16: Document to Target Audience Mappings 136
Table 17: NIST Capability to Research Capability Mapping 137
Table 18: AGELIGHT to NIST Document Mappings 141
Table 19: AGELIGHT Secure Data Storage & Transmission Summary 143
Table 20: AGELIGHT Secure Interface Management Summary 145
Table 21: AGELIGHT Secure Update Mechanism Summary 146
Table 22: AGELIGHT Overall Summary 146
Table 23: BITAG to NIST Document Mappings 147
Table 24: BITAG Common Section 7.1 Summary 149
Table 25: BITAG Common Section 7.2 Summary 140
Table 26: BITAG Secure Data Storage & Transmission Summary 152
Table 27: BITAG Secure Interface Management Summary 153
Table 28: BITAG Overall Summary 154
Table 29: CSA Document to NIST Document Mappings 155
Table 30: CSA Logical / Physical Identifiers Summary 156
Table 31: CSA Secure Software Configuration Summary 156
Table 32: CSA Secure Interface Management Summary 158
Table 33: CSA Overall Summary 158
Table 34: CSDE Document to NIST Document Mappings 159
Table 35: CSDA Logical / Physical Identifiers Summary 160
Table 36: CSDE Secure Data Transmission & Storage Summary 162
Table 37: CSDE Secure Interface Management Summary 163
Table 38: CSDE Secure Update Mechanism Summary 164
Table 39: CSDE Cybersecurity State Awareness Summary 164
Table 40: CSDE Overall Summary 165
Table 41: CTIA Document to NIST Document Mappings 166
Table 42: CTIA Logical / Physical Identifiers Summary 167

Table 43: CTIA Secure Data Storage & Transmission Summary 168
Table 44: CTIA Secure Interface Management Summary 169
Table 45: CTIA Secure Update Mechanism Summary 170
Table 46: CTIA Cybersecurity State Awareness Summary 179
Table 47: CTIA Overall Summary 171
Table 48: ENISA Document to NIST Document Mappings 172
Table 49: ENISA Logical / Physical Identifiers Summary 173
Table 50: ENISA Secure Software Configuration Summary 173
Table 51: ENISA Secure Data Storage & Transmission Summary 175
Table 52: ENISA Secure Interface Management Summary 176
Table 53: ENISA Secure Update Mechanism Summary 177
Table 54: ENISA Cybersecurity State Awareness Summary 178
Table 55: ENISA Overall Summary 178
Table 56: ETSI Document to NIST Document Mappings 179
Table 57: ETSI Common Sections Summary 180
Table 58: ETSI Secure Data Storage & Transmission Summary 181
Table 59: ETSI Secure Interface Management Summary 182
Table 60: ETSI Secure Update Mechanism Summary 183
Table 61: ETSI Cybersecurity State Awareness Summary 183
Table 62: ETSA Overall Summary 184
Table 63: GSMA Document to NIST Document Mappings 185
Table 64: GSMA Common Section 6.12 Summary 186
Table 65: GSMA Logical / Physical Identifiers Summary 187
Table 66: GSMA Secure Data Storage & Transmission Summary 188
Table 67: GSMA Secure Interface Management Summary 190
Table 68: GSMA Secure Update Mechanism Summary 190
Table 69: GSMA Cybersecurity State Awareness Summary 191
Table 70: GSMA Overall Summary 191
Table 71: IEC Document to NIST Document Mappings 193
Table 72: IEC Common Section Summary 194
Table 73: IEC Secure Software Configuration Overview 195
Table 74: IEC Secure Data Storage & Transmission 196
Table 75: IEC Secure interface Management Summary 197
Table 76: IEC Secure Update Mechanism Summary 198
Table 77: IEC Cybersecurity State Awareness Summary 199
Table 78: IEC Overall Summary 199
Table 79: IIC Document to NIST Document Mappings 201
Table 80: IIC Common Section 7.3 Summary 202
Table 81: IIC Common Section 7.6 Summary 203
Table 82: IIC Common Section 7.7 Summary 204
Table 83: IIC Common Section 11.5 Summary 204
Table 84: IIC Logical / Physical Identifiers Summary 205
Table 85: IIC Secure Software Configuration Summary 206
Table 86: IIC Secure Data Storage & Transmission Summary 207

Table 87: IIC Secure Interface Management Summary 208
Table 88: IIC Secure Update Mechanism Summary 208
Table 89: IIC Cybersecurity State Awareness Summary 209
Table 90: IIC Overall Summary 209
Table 91: IoTSF Document to NIST Document Mappings 211
Table 92:IoTSF Common Section 2.4.7 Summary 212
Table 93: IoTSF Logical / Physical Identifiers Summary 213
Table 94: IoTSF Secure Software Configuration Summary 214
Table 95: IoTSF Secure Data Storage & Transmission Summary 215
Table 96: IoTSF Secure Interface Management Summary 216
Table 97: IoTSF Secure Update Mechanism Summary 217
Table 98: IoTSF Cybersecurity State Awareness Summary 217
Table 99: IoTSF Overall Summary 218
Table 100: OTA Document to NIST Document Mappings 219
Table 101: OTA Logical / Physical Identifiers Summary 220
Table 102: OTA Secure Data Storage & Transmission Summary 221
Table 103: OTA Secure Interface Management Summary 222
Table 104: OTA Secure Update Mechanism Summary 223
Table 105: OTA Overall Summary 223
Table 106: NEMA Document to NIST Document Mappings 224
Table 107: NEMA Secure Interface Management Summary 226
Table 108: NEMA Secure Update Mechanism Summary 226
Table 109: NEMA Cybersecurity State Awareness Summary 227
Table 110: NEMA Overall Summary 228
Table 111: OCF Document to NIST Document Mappings 229
Table 112: OCF Common Section Summary 230
Table 113: OCF Logical / Physical Identifiers Summary 230
Table 114: OCF Secure Software Configuration Summary 231
Table 115: OCF Secure Data Storage & Transmission Summary 232
Table 116: OCF Secure Interface Management Summary 233
Table 117: OCF Secure Update Mechanism Summary 233
Table 118: OCF Cybersecurity State Awareness Summary 234
Table 119: OCF Overall Summary 234
Table 120: PSA Document to NIST Document Mappings 235
Table 121: PSA Common Sections Summary 237
Table 122: PSA Secure Software Configuration Summary 238
Table 123: PSA Secure Data Storage & Transmission Summary 239
Table 124: PSA Secure Interface Management Summary 239
Table 125: PSA Secure Update Mechanism Summary 240
Table 126: PSA Cybersecurity State Awareness Summary 241
Table 127: PSA Overall Summary 241
Table 128: NIST Function to IoT Capability 257
Table 129: Identity Function Categories to IoT Capability 258
Table 130: NIST Framework Function, Category and Code Overview 266

Table 131: NIST Identity Function to IoT Capabilities 267
Table 132: NIST Identity Function to IoT Capabilities and Research Findings 273
Table 133: NIST Detect Function to IoT Capabilities and Research Findings 280
Table 134: Detect Respond to IoT Capabilities and Research Findings 283
Table 135: Recovery to IoT Capabilities and Research Findings 287

Table of Figures

Figure 1: IoT Paradigms, Adapted from (Atzori, Iera, & Morabito, 2010). 23
Figure 2: Comparison of Cloud Offering Paradigms, Adapted from (Watts, 2017) 30
Figure 3: Postscapes IoT Protocol Overview 33
Figure 4: Kaspersky Labs IoT Malware Samples, Adapted From (Kuzin, Shmelev, & Kuskov, 2018) 36
Figure 5: Hype Cycle, Adapted from (Steinert & Leifer, 2010) 38
Figure 6: Construction of a Conceptual Framework, distilled from Creswell, 2014; Ravitch, 2017; Rogers, 2016 and Yin, 1994 61
Figure 7: A Model of the Discipline of Information Systems, Adapted from (Shanks et al, 1993). 63
Figure 8: A Single Case Study 70
Figure 9: A Multiple Topic Case Study 70
Figure 10: A Multiple Case, Multiple Topic Case Study 71
Figure 11: Proposed Multi-Embedded Case Study Research Design 75
Figure 12: Overall Research Design of Cases 83
Figure 13: Case 1, IoT Networks/Systems Overview 85
Figure 14: Case 2: Cybersecurity Principles Overview 87
Figure 15: Case 3: Socioeconomic Impact Overview 93
Figure 16: Case 4: Consumer Overview 94
Figure 17: Case 5: Enterprise Overview 95
Figure 18: Current Case Location in Overall Research Design 100
Figure 19: Internet of Things, Language Interpretation 107
Figure 20: Industrial Internet of Things: Component, Context, Sense & Reference 112
Figure 21: Cyber Physical Systems: Component, Context, Sense & Reference 111
Figure 22: Smart Cities: Component, Context, Sense & Reference 113
Figure 23: Ubiquitous Computing: Component, Context, Sense & Reference 114
Figure 24: Internet of Medical Things: Component, Context, Sense & Reference 115
Figure 25: Healthcare Internet of Things: Component, Context, Sense & Reference 116
Figure 26: Internet of Health Things: Component, Context, Sense & Reference 117
Figure 27: IoT Categorisation Schema 119
Figure 28: Case 2-A Location in Research Design 124
Figure 29: Overview of IoT Standard Capabilities 137
Figure 30: Document Characteristic Strengths Matrix (Green = Strong, Orange = Average, Red = Weak) 243
Figure 31: IoT Overlay Framework Construction 290
Figure 32: IoT Security Overlay Framework Example Workflow 291
Figure 33: Ideal Framework Implementation 302
Figure 34: NIST Framework Implementation 303
Figure 35: IoT Framework Implementation Flow 304

Figure 36: Research Artifact Usage ... 305
Figure 37: IoT Security Overlay Framework Stepped Workflow ... 306
Figure 38: IoTSoF Practical Implementation Workflow Expansion: Step One - Start ... 307
Figure 39: IoTSOF Workflow Expansion - Step Two: Framework Requirements ... 308
Figure 40: Step 3 - IoTSOF Workflow Expansion – Assess IoT Device Limitations ... 309
Figure 41: Framework Function Implementation Workflow ... 314
Figure 42: IoTSOF Sub-Category Workflow Components ... 315

1 INTRODUCTION

In this digital age, the increasing convergence of computing and telecommunication resources allows for greater connectivity of devices and facilitates the emergence of new computing paradigms. Computing packages and transistor counts have followed Moore's Law (Moore, 1998) and given rise to small, power-efficient chips allowing computing to pervade all aspects of life. These power-efficient chips have allowed for the creation of small, multi-function sensors. Such sensors have as many applications and forms as there are ideas, from complex Cyber-Physical Systems (CPS) that create 'smart cities' (Cassandras, 2016) to healthcare sensors and specialised wireless networks (Fernandez & Pallis, 2014; Pasha & Shah, 2018). IoT based sensors and their applications contribute to the increasing interest in the 'Internet of Things' (IoT) paradigm.

As new devices and information technology systems are developed and implemented, the security of these interconnected systems becomes paramount, with cybersecurity now a cornerstone of information technology operations – which is commonly defined as "measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack" (Cains et al., 2022). Despite this focus on cybersecurity within modern communication systems, these protections are still not well applied - breaches to international corporations and governments occur with alarming regularity. This poor application of cybersecurity protection remains an issue and is not limited to IoT - traditional systems are still frequently affected, often on a massive scale. Some demonstrations of this is the 7 Million Dollar Ethereum Crypto-Currency Hack (Wieczner, 2017), the Amazon S3 Web-Bucket Storage breach (Vickery, 2017), the Ascellion FTA hack exposing 3.51 million healthcare records (Alder, 2021). and the Florida Healthy Kids Corporation breach exposing 3.5 million healthcare records (Alder, 2021). In 2021 alone, more than 44.9 million healthcare records were known to be exposed by the Department of Health and Human Services' Office for Civil Rights' portal (Alder, 2021).

These attacks are not new phenomena. Cybersecurity breaches occur regularly, yet only the most damaging and high-profile ones are publicised. Examples of such historical breaches include the Sony Hack, exposing internal company data and personal information (Wagstaff, 2014), the Uber breach (Wong, 2017) and Yahoo ("2013 Hack", 2017) demonstrate the consequences not only on corporations, but individuals. Such attacks, either organised or opportunistic, are only increasing in frequency and impact.

1.1 The Current State of The Internet of Things

Kevin Ashton first coined the term IoT in 1999 regarding supply chain management (Ashton, 2011). Although the term has been around for two decades, the IoT does not yet have an accepted, singular definition. This lack of a definition is perhaps best exemplified by the existence of a document by The Institute of Electrical and Electronics Engineers (IEEE), titled 'Towards a Definition of the Internet of Things' (Abyi, 2015). As a 'living' document, it contains many definitions of what major companies, organisations and corporations believe the IoT to be, although the information is somewhat dated, with the latest revision published circa 2015. This convergence of ideas does not limit itself to the definitions of what IoT stands for – it expands to cover all aspects of this emergent computing paradigm. System boundaries and architecture, communication protocols, hardware, and differing approaches to IoT manifest as a highly diverse ecosystem. The application of cybersecurity becomes a unique challenge on an evolving platform, made critical by the scope and interconnectivity of IoT devices and their rapid, widespread adoption.

According to The Global System for Mobile Communication (GSM) Association (GSMA), up to 24 billion IoT devices were forecasted to be in use in 2020, generating an estimated $1.3 trillion in revenue opportunities (The GSM Association, 2016). This growth has continued, with estimates as high as 100 billion devices connected by 2025, generating near $10 trillion in revenue (Wood, 2017). Whilst this is based on the potential exponential growth of a new market segment, this illustrates the level of expectation present in the developing IoT ecosystem, with the rapid growth and adoption leading to new forms of revenue generation and driving further research and development. Thus, new market segments may continue to emerge as the platform evolves, leading to a further increase in revenue-generating ventures and producing an even greater number of devices.

As a result of this rapid growth and adoption, the IoT ecosystem currently suffers from an inherent lack of any unified approach to security at any level – be it device or across the ecosystem. While most aspects of traditional cybersecurity need to be considered, there are specific challenges in IoT. These challenges include the incorporation of low powered devices, physical access difficulties, new protocols, disparate transmission mediums, and device management. Whilst not an exhaustive list, this highlights the scope of the challenges, and indeed, the scale and rapidity of adoption indicates how critical it is to 'get it right'.

The number of devices that can be classed as IoT (or a derivative thereof) that currently exist is well into the billions and is growing at a near exponential rate. Given the proliferation of devices, data collection and data transmission are a particular focus for cybersecurity efforts. The analysis of such large volumes of data are within the purview of 'Big Data' and constitute problems of a different variety. As such, the analysis, storage, or other issues known to exist in the 'Big Data' paradigm are not within the scope of this research.

1.2 The Healthcare Internet of Things and the associated problem

The 'Healthcare Internet of Things' (HIoT) applies the IoT paradigm to many aspects of healthcare. This application ranges from clinical usage in hospitals to personal monitoring devices used every day. This creates a diverse range of devices, ranging from highly regulated clinical and medical devices subject to oversight and regulation in developed nations to the (relatively) less regulated commercial market. The market for HIoT devices was expected to reach $117 billion by 2020 (McCue, 2015) and involve 26 billion devices (Kvedar, 2016) – providing an almost direct correlation to non-health-related, more standard IoT devices.

The drive for IoT devices comes from a potential two-fold benefit for clinical settings. Firstly, the devices will become cheaper than many conventional options (Islam et al., 2015), and secondly, they provide greater flexibility and productivity in the healthcare environment. The possibility of greater quality of care across healthcare providers can result in a shift in the outlook of traditional healthcare. This diversity in care options allows for the expansion and investigation of more diverse concerns, such as 'ageing in place' (sometimes called Ambient Assisted Living), which benefits immensely from the application of HIoT devices (Aced López et al., 2015). The benefits across the field of digital health cannot be discounted, despite the weaknesses that are inherited by IoT (incorporation of low powered devices, physical access difficulties, new protocols, disparate transmission mediums, and device management).

Cybersecurity is critical when applied to HIoT, as the consequences of malfunction or compromise are magnified by the direct interaction with people and their health. For example, if a pacemaker malfunctions or is compromised, it is not only the device that has an issue – the person it resides in has a genuine chance of severe consequences, even death (Cybersecurity and Infrastructure Security Agency , 2021).

Despite the positive and negative aspects inherited from IoT, HIoT contains its own unique challenges. Highly regulated and controlled, with strict privacy and operations laws, traditional medical devices have long been proprietary, stand-alone, and minimally connected. Coupled with the complicated workflows of a healthcare environment, the new HIoT devices are no longer segregated from each other. They are parts of the overall system comprising of patient, clinician, technology, and processes (S. Campbell, 2010). The traditional approach of physically segregated networks (Cooper, 2008) is no longer relevant. Instead, modern healthcare systems have converged, taking advantage of communication technologies like Wi-Fi (Cooper & Fuchs, 2013) mean that devices are now logically separated using virtualized networking technologies. This change in networking architecture and the move toward shared mediums, dramatically increases the difficulty in applying effective cybersecurity to these devices and the networks they operate on (Williams & McCauley, 2016).

The increased difficulty in the application of cybersecurity does not diminish the benefits gained from implementing HIoT technology, both in terms of cost benefits and, more importantly, the increased level of care provided to patients, both clinical and non-clinical. This means that finding a solution for the security challenges is more urgent than with standard IoT – especially when, as previously discussed, consequences of malfunction or compromise can directly impact a person's health (Cybersecurity and Infrastructure Security Agency, 2021). These factors, along with the need for regulatory oversight, means that health devices existing on shared transmission mediums now face additional challenges that are not present within a comparative non-medical network. This is detrimental to preventing cybersecurity incidents, especially since these devices were previously designed to perform in a stand-alone, semi or fully isolated capacity before IoT integration.

The previous standalone approach meant that security was not always considered a priority or critical component. With the influx of devices based on new technology, protocols and mediums, and these new technologies sharing network space with other non-health-related traffic, the application of cybersecurity becomes critical, especially given the sensitivity of the data and the possible risk of an incident translating to patient harm. Therefore, this research aims to address this problem by creating a framework for cybersecurity that can be applied to this dynamic area to guide a suitable level of cybersecurity protection.

2 LITERATURE REVIEW

This literature review of the IoT ecosystem and its associated cybersecurity challenges is presented in the following order. Firstly, an exploration of the current linguistic challenges around the term IoT and all inheritor ecosystems is presented, highlighting the language difficulties that a rapidly evolving ecosystem can have. Addressing these (language) issues, the current understanding of the IoT and HIoT ecosystems is discussed, along with an overview of applicable cybersecurity measures. Finally, the current issues with each ecosystem and the potential solution avenues are addressed.

IoT is rapidly approaching the status of a standard facet of Information Communication Technology (ICT) employed by a wide range of entities (Gluhak, 2016). These entities range from utility companies utilising smart meters to track utility usage (Yilin Mo et al., 2012), streamline operating costs to building monitoring systems that track estimated utilisation, and to wearable sensors to assist in delivering healthcare applications (Chiuchisan et al., 2014). The demands and drive to consume and create these devices, technologies and applications is as diverse as the possible applications.

IoT crosses traditional boundaries of computing and has become an amalgamation of many different computing approaches, with cloud computing at the forefront. Incorporating the new uses of existing developments, terminologies, and technologies, along with the brand-new applications, has generated opportunities and challenges. These challenges are also present within the traditional (non-IoT) computing space and cover everything from management and standardisation to cybersecurity (Russell & Duren, 2016). A key interest of this research is the known difficulty in IoT cybersecurity stemming from this combination of new and old technologies colliding in the same sphere of operation.

This large and diverse area of the IoT creates a unique blend of technology, human interaction, and automation, under constant and rapid evolution. This evolution is driven by modern marketing, social media virality (organic interest) and global commerce all influence possible new devices. This rapid development is limited only by ingenuity as new technological advances have enabled greater ease in creating an IoT device. Devices are getting smaller and more computationally powerful as time progresses, integrating more capabilities. This limit or blurring of what IoT is, can be and will become has caused rapid fracturing of the IoT ecosystem, difficulties in obtaining a whole of ecosystem outlook and potential cybersecurity issues. These factors are some of the major driving factors behind the increase in regulatory interest by special interest groups, industry, and government.

Rapid development brings with it sacrifices, and the application of cybersecurity is usually the first casualty. This lack of cybersecurity is exacerbated by the convergence of hardware and software creating more interdependent systems, where the line between hardware and software is increasingly blurred. This blurring of hardware and software has created more interlinked systems, resulting in magnified cybersecurity vulnerabilities, and increases the difficulty in gauging the potentially far-reaching impacts of an incident.

Despite these drawbacks, IoT is gaining more traction and is firmly believed to be a solution for some of the dynamic problems in modern communication and data usage, where efficiency is just as important as performance (Lv et al., 2021; Sharda et al., 2021; Zhan et al., 2021).

2.1 TERMINOLOGY CHALLENGES

The language used to describe the diverse areas of IoT and HIoT is expanding. This is caused by the rapid expansion of research and development in the area – as each solution is developed, there is no standardised naming schema, and new terms are invented – creating a state of flux.

The use of language in modern society is fundamental to understanding anything and everything. We describe and define things through language, and through these boundaries come to an understanding that is universal for everyday usage. This can be demonstrated technically by creating an ontology, as ontologies are identified as a knowledge base applicable to a specific context (Uschold & King, 1995).

A universal understanding allows for people to communicate and understand what a specific topic is, what it contains, what it does not contain and what is related (Skuce, 1995). When new technologies, fields of study or items are created – this process begins. Such definitions need to evolve through language – they take time, effort, and many iterations of refinement. Through these iterations, the boundaries, definitions, and descriptions change until eventually, they settle on agreed definitions and boundaries.

While this is a continually iterative process, the current language to describe HIoT is fractured. Different organisations have slightly different interpretations, and with an absence of the agreed-on definition, complete with boundaries, the interpretation of these exploratory definitions also shift. Each person investigating the field may generate a new term, repurpose an old one to describe a new approach, adapt the terminology and phrasing from a similar field to describe a new IoT, and other divergent aspects of language development.

This process causes the language to fracture. Whilst this may not cause issues for the everyday use of the term, problems can arise when clear definitions and boundaries are required – as in cybersecurity. This fracturing of language can be seen within IoT and its derived technologies. IoT has become the 'de-facto' term for referencing the area (Berte, 2018); however, it is not the only term, and there are many synonyms and connected phrases – such as Industrial IoT, Internet of Stuff, Connected Things, and so on, as this is not intended to be an exhaustive list.

The lack of non-standard terminology is also problematic when undertaking research. For example, suppose one wishes to research particle physics. In this case, there are defined terms that will return literature on whatever sub-section of the topic you are looking at, as they are clearly defined, described, and standardised. The opposite is true for newer areas like the Healthcare IoT, where terms are still developing and somewhat fluid (Berte, 2018).

To investigate this area for any meaningful research, the first step is to ascertain the language used to describe the topic. As IoT and HIoT are newer fields, are constantly evolving as new techniques are tried, tested, and summarily adopted or discarded; the language to describe this area is also evolving. Whilst this step of linguistic investigation is undertaken for every piece of research, the difficulty increases steeply when the terms shift during the investigation.

HIoT is a multidisciplinary field, and the terminology is drawn heavily from medical terms as well as existing medical and regulatory domains. This makes the language utilised both familiar and divergent when attempting to capture the literature on IoT and associated technologies.

2.2 IoT Perspectives

The following section presents the current understanding of IoT and subsequently HIoT. There are three main paradigms or 'visions' that make up the current state of IoT – "internet", "semantic" (data), and "things". These are summarised in Figure 1.

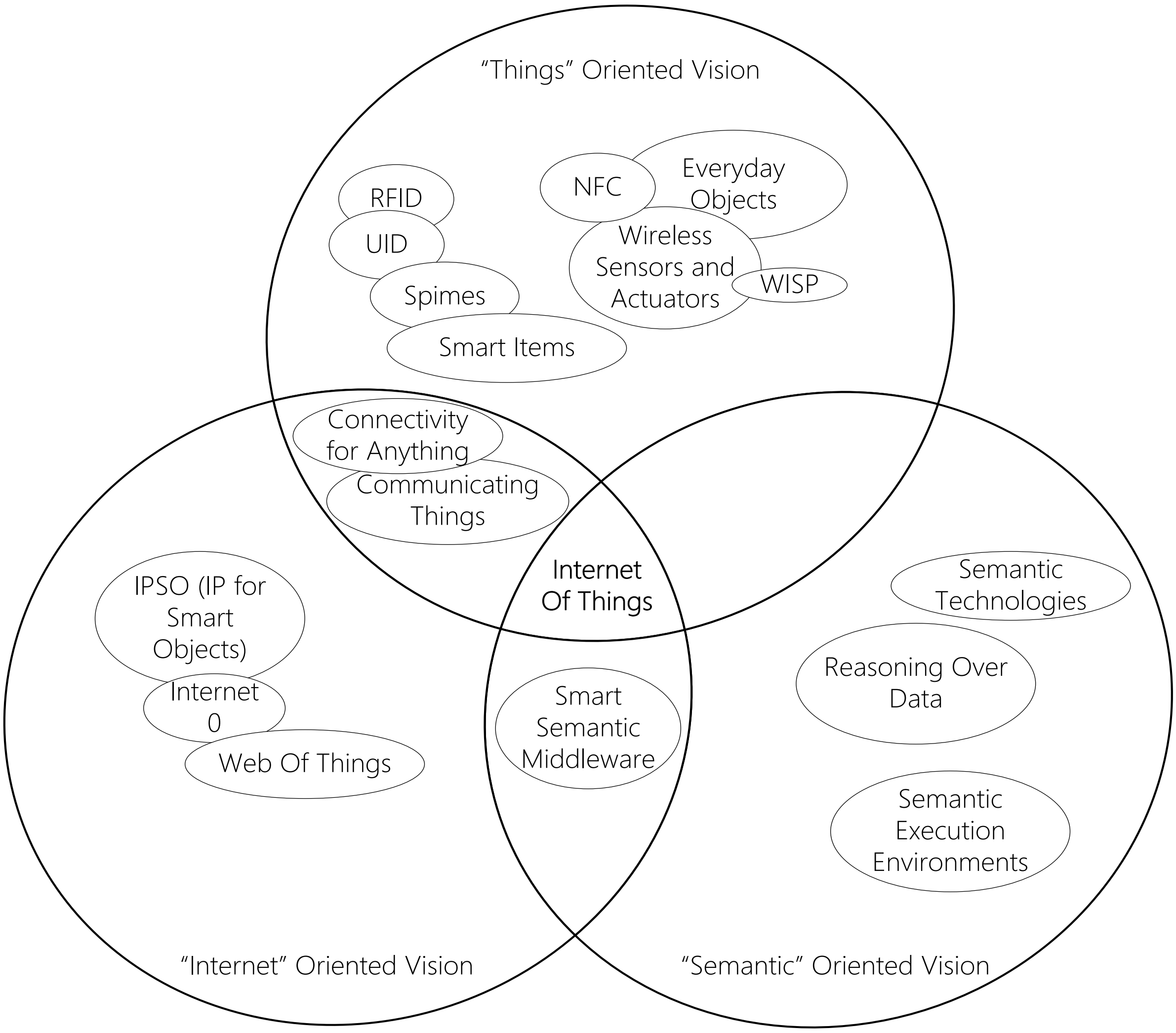

"Things" Oriented Vision
RFID
UID
Spimes
Smart Items
NFC
Everyday Objects
Wireless Sensors and Actuators
WISP
Connectivity for Anything
Communicating Things
Internet Of Things
IPSO (IP for Smart Objects)
Internet 0
Web Of Things
Smart Semantic Middleware
Semantic Technologies
Reasoning Over Data
Semantic Execution Environments
"Internet" Oriented Vision
"Semantic" Oriented Vision

Figure 1: IoT Paradigms, Adapted from (Atzori, Iera, & Morabito, 2010).

The *things* based vision is concerned with utilising physical hardware to perform a task, which may be embedded sensors as part of a Cyber-Physical System (CPS), or actuators as part of an Industrial Control System or Home Automation sensors. The scope of this paradigm covers a breadth of devices – each with its own unique characteristics. The extensive scope, rapid development and deployment of devices means that cybersecurity, whilst acknowledged as a requirement, may not be implemented correctly or at all.

The interconnectivity of IoT ties into the *internet* vision presented in Figure 1. This vision focuses on the connectivity of devices to each other and to a larger system. Within this vision, there are multiple aspects as concurrent ideas are pushing forward – some directly created for IoT environments, some not. For example, the Machine-2-Machine (M2M) platform covers communication between devices to fulfil tasks with minimal or no human input (Abyi, 2015).

The development of this aspect (M2M) is generally focused on CPS; however, the technologies are applied outside of their originating areas. The application outside of intended design scope is a common action associated with IoT. These new devices have rendered the existing traditional approaches, applications and some tooling used to apply cybersecurity impotent (Ahmed et al., 2020; Dhirani et al., 2021; Giaretta et al., 2019).

The interconnected *things* drive the vision of *semantics*, including the effective usage of the data that these sensors can provide. These sensors can tie into Big Data for advanced analytics and smart execution environments (Z. Khan et al., 2015). The *semantic* outlook of IoT concerns itself the presentation, description, and processing of interconnected device to allow for intelligent actions with limited to no human contact (Pandey et al., 2021). This *semantic* helps in the creation of IoT based ontology frameworks, for example the "Semantic Sensor Network Ontology", used to describe the "…sensors and their observations, the involved procedures, the studied features of interest, the samples used to do so, and the observed properties, as well as actuators" (Mark Schildhauer, 2016).

The three visions in the IoT paradigm share common concepts and ideas. To understand the magnitude of these systems, a level of abstraction is mandatory. This required abstraction has culminated in IoT taking advantage of newer computing paradigms – like cloud, edge, and fog computing. These paradigms are heavily integrated into all aspects of IoT and some forms of HIoT (Rahmani et al., 2018; Ren et al., 2017). Allowing access to devices from anywhere is a core aspect of IoT. This abstraction from the physical aspects to the logical layout of a network is counterproductive to the application of cybersecurity.

Given the combination of abstraction, new devices, new characteristics of new devices, new protocols, and associated communication processes are created to fill the gaps that are not adequately met by existing technologies. As IoT is still under active development, new communication protocols are continually being created and existing protocols expanded. The maturity, adoption, and usage of IoT all play a role in how secure these new and upgraded protocols are.

From the first mention of IoT, several different terms have appeared to further sub-divide the umbrella term of the IoT; Anything, Anywhere, Anytime (A3), Machine-2-Machine Communication (M2M) and Cyber-Physical systems (CPS) with more appearing as new technologies are devised.

The idea of A3 is the initial drive that aims to make objects smart and independently communicable. The A3 concept itself is not new and it is also known as Ubiquitous Computing (UQ/UBC), which has been in existence since the early 2000s (Lyytinen & Yoo, 2002). The A3 or UQ concept can be seen as the core idea of the IoT, as it aims to connect everything to everything else. M2M communications can facilitate this connection and smart decision making.

M2M communication is the concept that devices can dynamically communicate and make decisions without external (human) input. Applications of M2M allow for complex systems that can operate in both a standalone manner and as part of a greater system. Some of this logical decision making is cojoined with the vision of CPS, where systems are automated to some extent.

CPS covers another aspect of IoT, and parallels can be drawn between it and existing Supervisory Control and Data Acquisition (SCADA) networks – systems used to control and monitor industrial processes (Gao et al., 2014). As CPS focuses on "physical and engineered systems, whose operations are monitored, coordinated, controlled, and integrated by a computing and communicating core" (Rajkumar et al., 2010), they can be equated to the next generation of SCADA - taking inspiration from both A3 and M2M to achieve this.

CPS focus on physical interaction means that these systems are utilised industrially. This creates a virtual exposure that was, in past generations, not present. As CPS moved towards managing utilities (e.g., power, water, and gas), sluice gates and other physical objects, the possibility of a critical disruption due to malicious interaction, user, or software error dramatically increased. This increased the total attack surface of networks with such integrations, due to interfacing IoT devices with real-world interactions (Sadeghi et al., 2015). This problem is shared with older, existing SCADA networks. The security of these networks, where the protocol and hardware were put into place decades ago, remains a critical infrastructure vulnerability, and many of these hurdles are inherited by CPS (Francia III et al., 2012; Gao et al., 2014; Munro, 2008).

When comparing these similar yet divergent aspects of IoT, the issues at the base of the technological tree will be inherited by any technologies derived from it. This inheritance is also present in HIoT, where new technologies created in IoT allow for new healthcare dynamics (Miranda et al., 2016).

2.2.1 HIoT

Each part of the existing digital health umbrella - including digital health, eHealth, mHealth, telecare, telehealth, and telemedicine (Salem, 2016) contains an aspect or implementation of HIoT. This application of IoT technology to health aims to enable new aspects of healthcare and improve existing ones. An example is smart sensors and embedded software systems that can form part of larger software suite. This application falls under the umbrella of Software as a Medical Device (SaMD) (Ludvigsen et al., 2022). To date, SaMD has been limited to systems excluding IoT, and thus HIoT will expands the scope of SaMD, as it moves toward larger and more sophisticated software systems (Carroll & Richardson, 2016).

However, as previously stated, the problems with the base IoT ecosystem are inherited by any expansion on it. These inherited problems are compounded by additional oversight, regulatory and privacy constraints for healthcare and a result of the potential risk of human harm due to incorrect operation of a device.

2.3 IoT Technologies

The technologies used when implementing IoT are not restricted to any one specific set of technology. All aspects of ICT are adapted to, or created for, IoT. This means that there are new applications of existing technologies for IoT, like Radio-Frequency Identification (RFID) and Near-Field Contact (NFC) and new concepts, like vehicle-to-vehicle (V2V) communications (Shah & Yaqoob, 2016).

2.3.1 Infrastructure

The networking infrastructure of IoT deployment can be significantly different form existing networks – the scale of the devices, their locations, communications restrictions, and data processing all create a set of unique challenges. IoT relies on our existing and understood networking paradigms, like Cloud Computing (Rani & Gill, 2019). As with all technologies and ideas, the areas where the existing approaches do not provide the required functionality must be identified.

2.3.1.1 *Networking*

The IoT platform and general system layout can be loosely aligned with the existing classical computing deployment patterns of Cloud, Hybrid and Virtual. Whilst each of these deployment patterns draws from the existing computing architectures, with modifications to the deployment occurring to align with the requirements of IoT. Even with the solid base of traditional computing, the network designs of Cloud, Hybrid and Virtual deployments are in constant flux as new devices and technologies are developed and used. In shorter terms, the communication networks inherit the same base issues as IoT; extensive, rapid evolution.

Overall, it can be said that there is a definite shift to cloud providers, with the forefront of this shift occurring around the late 2000s and early 2010s (Aljabre, 2012; Plummer et al., 2008). Microsoft Azure and Amazon Web Services are two of the significant providers of IoT Platform options. Cloud architecture itself is a well adopted and tested option and is firmly integrated into Enterprise ecosystems. The implementation of cloud technologies can be roughly divided into four different deployment types: On-Site, Hybrid, Cloud and Virtual (Fernandez & Pallis, 2014). Whilst by no means the definitive list, this is sufficient to identify issues and possible gaps in IoT cybersecurity approaches and the unique challenges within different deployments.

2.3.1.1.1 On-Site Deployments

On-site deployment (also referred to as on-premises) is still a common type of service deployment. It provides an on-site datacentre resulting the most control of all aspects of the deployment; this also results the most amount of overhead (Hirali B., & Kansara, 2021). This deployment type is not limited to the servers or enterprise hardware, as businesses still provide services on site. The provisioning of employee hardware, network connectivity, and other managed services and maintenance becomes an overhead of the business.

This on-site deployment also allows for an arguably paradoxical strongest yet weakest application of cybersecurity. As all risk is taken by the company in this scenario - there is limited ability to offload responsibility, and all matters of operation are either handled in house or outsourced to obtain the requisite skillset. The potential losses can be highly damaging, in both financial costs and societal image (Wagstaff, 2014; Wong, 2017).

2.3.1.1.2 Cloud Deployments

Cloud deployments leverage external hardware, allowing organisations to offload some of both management and manpower overheads that on-premises deployments can incur. The rapid adoption of cloud services (occasionally called internet-enabled services) can be partially attributed to the reduction in overhead, and the flexibility afforded by cloud platforms (Hirali B., & Kansara, 2021). The flexibility of cloud lies in its ability to provision resources on demand and scale these resources both vertically, allocating more resources or horizontally, creating more instances.

2.3.1.1.3 Hybrid Cloud Deployments

The most common, with a combination of on-premises and cloud deployments. Organisations offload what is feasible for them to do so, aiming to reduce management overheads and risk levels (Hirali B., & Kansara, 2021). Usually, there is a monetary saving overall from the costs of services and no longer requiring the associated upkeep of utilities and hardware on-site.

2.3.1.1.4 Virtualized Deployments

Virtualised Deployment is not strictly a type of dedicated layout, as it is the application of virtualisation technologies to abstract the requirements and function away from physical hardware (Qadeer et al., 2020). This commonly takes the form of Software Defined Networking (SDN) to define a cohesive networking layer. This layout type is usually applied to secured cloud-based endpoints to enable transparent and secure communications between the cloud and other infrastructure. This layout comes with the same risks as either hybrid or pure cloud-based deployments, as depending on the deployment, as it is possible to cross boundaries of on-premises hardware and cloud resources. With this abstraction away from specific devices or hardware comes additional complexity, which must be managed. This need for repeatable, managed deployment of resources is related to Infrastructure as Code and its multitude approaches (Rahman et al., 2019).

2.3.1.2 *Critical Infrastructure*

As communication assets are now commonly included under the umbrella of critical infrastructure, IoT can both consume these assets and be a part of these systems. IoT is used to monitor the status of these systems and take advantage their capabilities. The extensive geographical coverage of critical infrastructure facilitates the deployment of IoT to more remote areas.

2.3.2 Platforms

The financial benefits of IoT and its subsequent rapid adoption and implementation has led to a diverse yet fragmented ecosystem. An example of this fragmentation is the lack of standard interoperability for IoT – instead a loosely defined set of patterns to facilitate communications has developed where the overall IoT ecosystem is dominated by vertical, fit for purpose deployments implementing proprietary or semi-proprietary systems. Given the original premise of a self-managing interconnected network (Ashton, 2011), progress towards this has not been apparent.

To illustrate the issues with interoperability, we can take the following services developed to facilitate IoT and acts as deployment and management platforms:

1. Amazon Web Services IoT
2. Microsoft Azure IoT
3. Google Cloud Platform
4. ThingWorx IoT Platform
5. IBM Watson IoT
6. Samsung Artik
7. Cisco IoT Cloud Connect
8. Hewlett Packard Universal IoT Platform

This is not a complete list of available platforms, with new platforms being developed and older ones being decommissioned. As each platform is competing with others in delivering similar services, choosing one platform over another becomes an issue of compatibility with existing services and infrastructure, as competitors rarely integrate well with one another. This integration difficulty has been noted by multiple studies, where user-to-device is simple and well understood, but platform-to-platform is both costly and challenging (Mineraud et al., 2016).

This difficulty in integration favours the creation of vertical deployments – where the devices are configured to fit specific deployment and platform requirements without concern for future interoperability. This is in almost direct opposition to IoT's true vision, with devices all communicating with one another seamlessly.

2.3.2.1 *The Internet as a Platform*

The delivery of business services has also evolved alongside the internet. Delivering services to consumers is now a significant and accepted way to enter marketplaces – this can be represented by the differing levels of access, control, and third-party management.

These levels are summarised in Figure 2 – as PaaS (Platform as a Service), IaaS (Infrastructure as a Service), SaaS (Software as a Service) – this graded offload of responsibility is sometimes called by the umbrella term XaaS (Anything as a Service). This segmentation of services into distinct layers allows opportunities for greater flexibility and the ability for businesses to reduce overheads associated with service management. When managing larger services, each individual layer below can account for multiple teams of people.

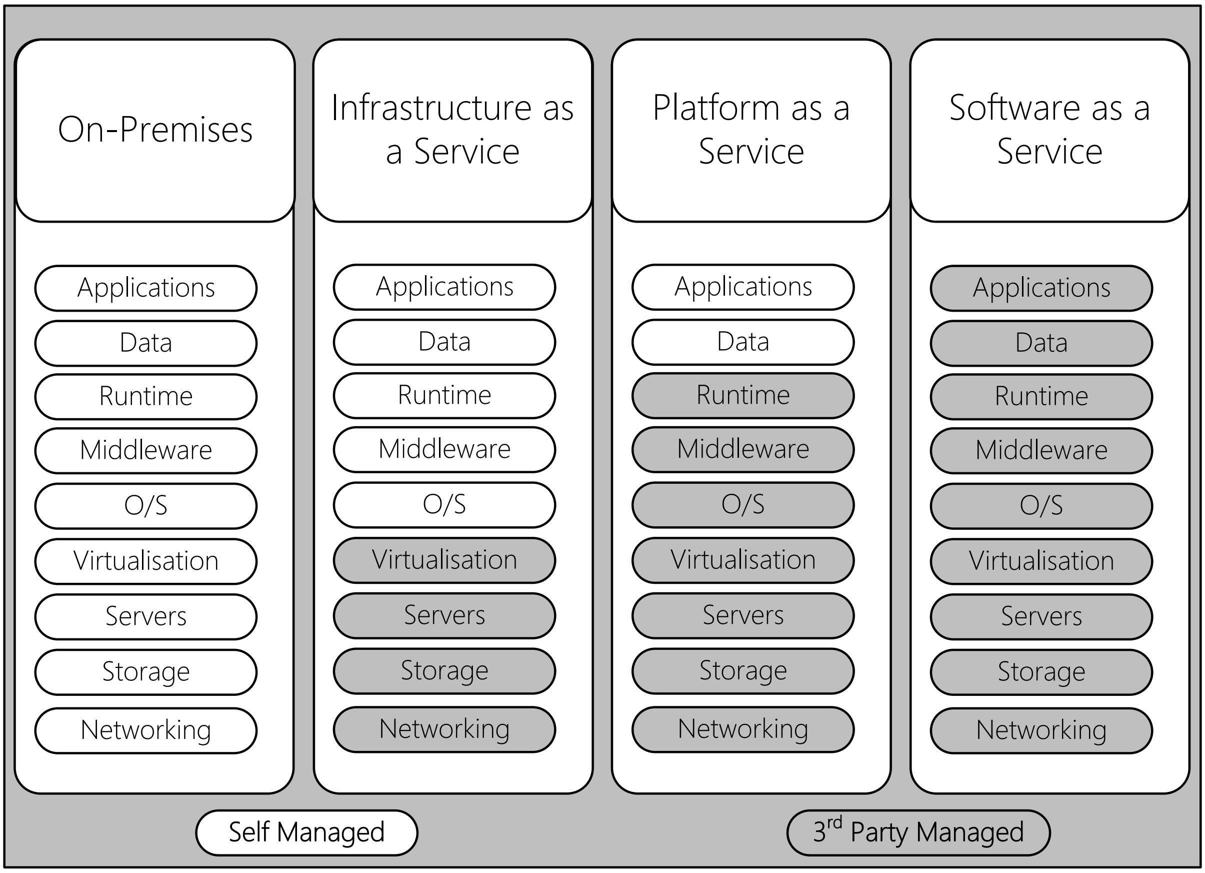


Figure 2: Comparison of Cloud Offering Paradigms, Adapted from (Watts, 2017)

This approach provides a new level of flexibility as operations can now be tied to a level of responsibility that suits the organisation, delegating the management to allow for more focus on the core focus of the organisation. The major cloud platforms, while not directly interoperable with one another, allow for integrations to cross the boundaries between the different providers with minimal issues. This is the opposite of IoT, where the ability to integrate across different platforms is significantly more difficult. It should be noted that the initial cloud offering suffered from the same issues of IoT- as the cloud platforms have matured, the ability to migrate and integrate between them has also matured.

This pattern of cloud-based technologies transfers some of the risk present within an organisations risk analysis but can results in larger breaches when a cybersecurity incident occurs. Of course, this risk offloading depends on the architecture that is implemented across an organisation, independent of organisational size and range.

PaaS is the most common type of deployment, with services provided by multinational technology corporations - Microsoft Azure, Amazon Web Services and Google Cloud Platform. These platforms also offer the IaaS and SaaS as part of their product profile, but this is in the minority for IoT deployments.

When utilising a cloud platform (PaaS), cybersecurity focuses on the deployed resources, not the platform. A section of the normal end to end cybersecurity is now handled by the PaaS company – like Distributed/Denial of Service (D/DoS) protections, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). These systems are still deployed as part of Defence in Depth, however, they become less effective or supplementary to other security techniques, given that the core of the network these systems operate on are no longer under the jurisdiction of the company deploying the tools.

2.3.3 Devices

Device adoption and new device development are driven by hype and technology factors discussed in section 2.4.2, Marketing and Consumer Expectations. New technologies are somewhat of a misnomer, as the technologies themselves are not always new – the application to differing fields that they were not initially designed for is the new aspect. Whilst this is a semantical point, many IoT technologies are existing technologies applied to IoT devices and problems. It is this application outside of initial design specifications that can also potentially cause cybersecurity issues.

In a follow-on from the hype cycle, the manufacturing market also drives the creation and implementation of new devices. Utilising the connectivity of modern communication markets and the increased saturation of technology in modern life has allowed the adaptation of older technologies to fulfill new purposes – a cost benefit to manufactures who can avoid costly retooling of production lines. This expansion of purpose versus design is not new to IoT, as parallels can be drawn to Bring Your Own Device (BYoD), where work and leisure can mix on a single device. The differences between IoT and BYOD mean that while they appear similar at first glance, the solutions needed to solve any cybersecurity and management problems can be drastically different between the two.

Devices in the current adoption push for IoT are usually first or second-generation devices – this means that they are either immature and can be seen as prototypes, complete with the unexpected bugs, glitches, and use-cases that first-generation devices will have – including existing security issues with embedded hardware or software.

2.3.4 Protocols

Legacy protocols are still deployed and, in some cases, are more than a quarter-century old. The MODBUS Protocol for Programmable Logic Controllers is an example of a legacy protocol from Modicon (now Schnieder Electric) – first released in 1979 and is still in usage with revisions as current as 2012 (The Modbus Organization, 2019). When designed, the need for digital security measures was minimal and generally not considered as a priority. This results in the inheritance of technical debt and security risks as protocols are applied to situations that they were not initially designed for – even with revisions to protocols attempting to patch or mitigate fundamental design omissions.

There are two aspects to describing the protocol issue – the number of protocols and the timeline of their introduction, adoption, and migration from legacy to current. Given the large breadth of devices and protocols in play, there are numerous overview guides and articles that describe a multitude of differing solutions. An example of one perception of protocol interconnectivity and scale is expressed in Figure 3.

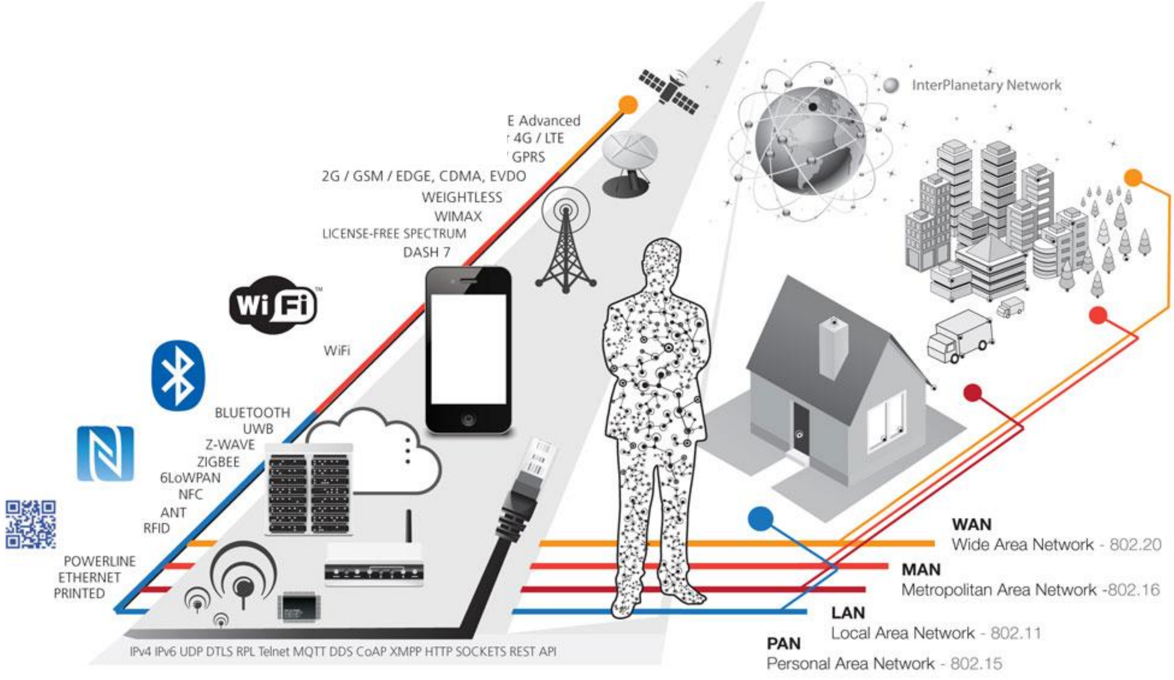

InterPlanetary Network
E Advanced
4G / LTE
GPRS
2G / GSM / EDGE, CDMA, EVDO
WEIGHTLESS
WIMAX
LICENSE-FREE SPECTRUM
DASH 7
Wi Fi
WiFi
BLUETOOTH
UWB
Z-WAVE
ZIGBEE
6LoWPAN
NFC
ANT
RFID
POWERLINE
ETHERNET
PRINTED
IPv4 IPv6 UDP DTLS RPL Telnet MQTT DDS CoAP XMPP HTTP SOCKETS REST API
WAN
Wide Area Network - 802.20
MAN
Metropolitan Area Network -802.16
LAN
Local Area Network - 802.11
PAN
Personal Area Network - 802.15

Figure 3: Postscapes IoT Protocol Overview (Postscapes, 2019. CC BY-NC-SA 4.0

The multilayered approach to protocols masks some of the important contextual differences in legacy equipment across IoT and its derivatives. Of the protocols in active use, many were created before cybersecurity was a consideration in design or deployment for these control networks – they were physically isolated (in most cases), leaving little need for extensive digital security measures. This applied primarily to critical infrastructure control systems. The same principle of legacy protocols and equipment can be applied to nearly every application of IoT that integrates with existing systems – inheriting the legacy issues of the protocol or device that, while not a problem when it was installed, has now become a security hole that can pose a significant risk.

Notably, legacy protocols are not just retired instantly – they are still present in some modern systems. These systems are (usually) real-time systems that cannot be powered down, patched, or altered easily (or if at all) once deployed. These systems can usually be found in critical infrastructure, raising the impact of potential disruption.

New protocols are generally followed by new devices that take advantage of the features provided by the new protocols. This results in a feedback loop – where a new protocol provides a specific feature that a new device can take advantage of, subsequently creating a new way to communicate using the new device and protocol. An example of this loop is the creation and improvement of the 802.11 Series of Standards – colloquially known as Wi-Fi. This looping, iterative improvement is not always backwards compatible with older devices – be it due to computing requirements, hardware, or software limitations.

2.4 IoT Usage

The environmental factors and cost reduction resulting from IoT are a significant driver to the adoption of new technologies and devices. For instance, the ability to monitor utility usage per floor and target inefficient building areas, and to track utilities usage (power/water/gas) and highlight areas for targeted resource consumption reduction. IoT is usually deployed as a monitoring system; the breadth of sensors – from water flow to personal tracking to geographical analysis allows for greater breadth of data to be captured, subsequently allow for finer detailed analysis (Attaran, 2017).

The drive to make processes smarter and more efficient creates an increasing demand for IoT, with near universal appeal to all facets of modern life – enabling new solutions to both old and new problems. This flows into service delivery, where increasing the *smartness* of the devices can enable data-based analytics to spot trends, issues and assist with more accurate forecasting.

This increase in smartness is valid across all industries and is not just limited to technologies. This smartness allows for financial and procedural benefits. In 2011, Cisco predicted that more than 50 billion devices would be connected in 2020, with an estimated marker worth of $1.4 Billion (Dave, 2011). This growth has continued, with a newer estimate of $1.38 Billion by 2025 (Al-Sarawi et al., 2020).

This growth in IoT and its adoption demonstrates the usefulness and relevance of IoT and that it will continue to be used. This increase in adoption also influences a change in networking layout – changing the requirements of how cybersecurity protections are to be applied.

2.4.1 History

Table 1: IoT Key Events Timeline presents an excerpt of the key events along the timeline of IoT. As such, the presentation of some key events highlighting the increase of technologies, adoption, applications, and cybersecurity events is presented – demonstrating the overall news coverage and visibility of the IoT ecosystem. As an example of this increasing number of events over time, Kaspersky Labs (Kuzin et al., 2018) published a report on malware usage in IoT attacks captured by their monitoring network.

Table 1: IoT Key Events Timeline

1980-2000	2001-2010	2010-Now
Uncorroborated reports of Trojan in SCADA system causing an explosion in Trans-Siberia gas pipeline (Weiss, 2008)	January 2003: Nuclear Power Plant Network infected by Slammer worm. (Poulsen, 2003)	August 2011: A smart 'Cow Monitoring System' (Steeneveld & Hogeveen, 2014)
March 2000: Sewage-Processing plant in Australia (Smith, 2001)	August 2003: The Blaster worm infected the communication system of the U.S. railway company (Guth & Machalaba, 2003)	May 2012, 'Flame' malware discovered (McElroy, 2012)
	September 2003: Nachi worm found in Government Production Network (Labott, 2003)	June 2012: IPv6 World Launch (*World IPv6 Launch*, n.d.)
	2005: First UN/ITU Report on IoT (ITU: The Internet of Things, 2005)	2012: Carna Botnet discovered (Internet Census 2012, 2015)
	August 2005: Zotob worm infects 13 US auto plants causing shutdowns and delays. (Robert, 2005)	2012: ICS Honeypots demonstrate speed and depth of cyber-attacks (Simoes et al., 2013)
	2006: Breach into PA water plant installation of spyware on plant's computer systems (McMillan, 2006)	December 2013 to January 2014: First Cyber-attack using 'Smart Devices'. (Proofpoint Uncovers Internet of Things (IoT) Cyberattack, 2014)
	January 2008: Commuter tram collision by glancing blow and derailment due to unauthorized switching (Layden, 2008)	March 2014: Industrial Internet Consortium (Hardy, 2014)
	2009: First Browser-Based Cloud Apps (Glotzbach, 2009)	October 2014: Number of Devices exceeds the number of people on earth (There Are Officially More Mobile Devices than People in the World, 2014).
	August 2009: First Wireless Network, Pacemaker (Gruber, 2009)	2014: US Hospital trials remote patient monitoring ("Exclusive" 2014)
	September 2009: First Cube Satellite (Noca, 2009)	May 2015: 2nd IoT World Conference and Exhibition

		with 4000 attendees 250 speakers and 150 exhibitors.
	September 2009, Utility smart meters are compromised in scale resulting in loss revenue	2018: Half of World internet traffic from non-pc devices. (Cisco Visual Networking Index, 2018)
	June 2010: Online Tide Monitoring System (Hans, 2010)	2018: Internet traffic from Wireless devices exceed that of wired (Cisco Visual Networking Index, 2018)
	June 2010: Stuxnet worm discovered (Farwell & Rohozinski, 2011)	

Figure 4 shows a significant increase in the interest and active attacks utilising IoT as a vector for cybersecurity compromise.

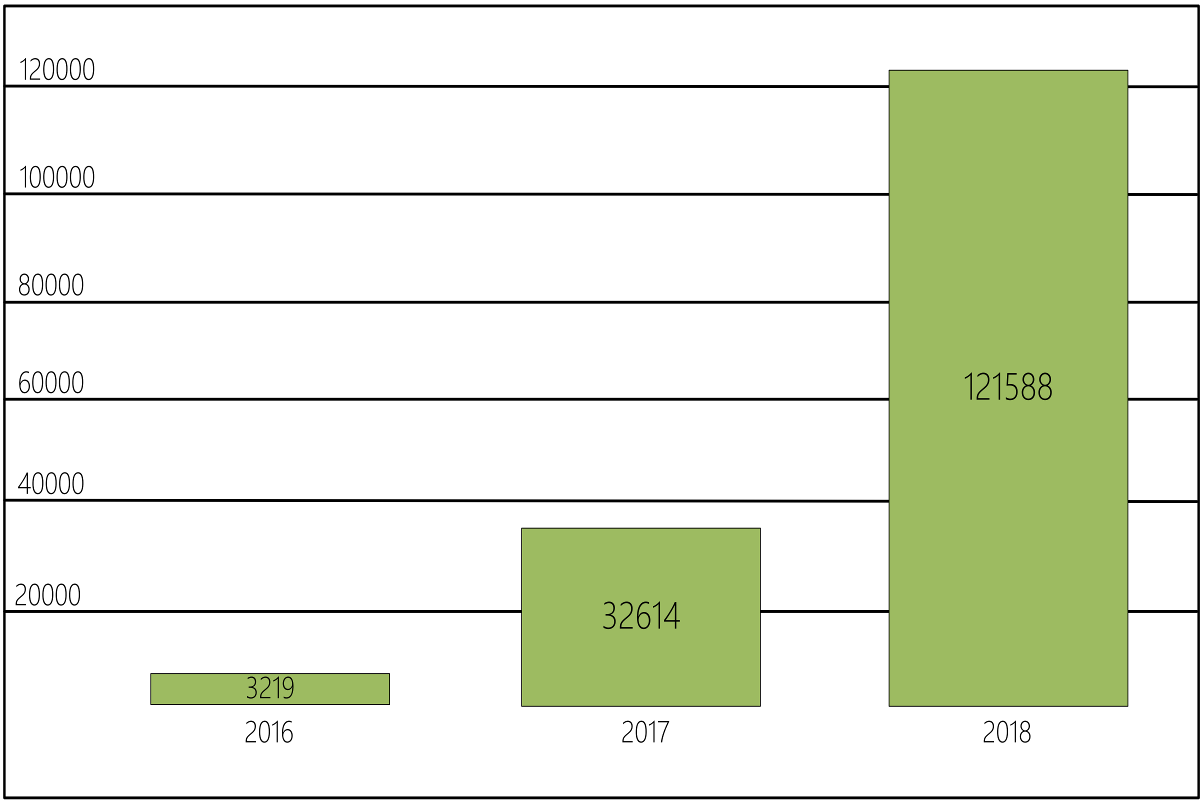


Figure 4: Kaspersky Labs IoT Malware Samples, Adapted From (Kuzin, Shmelev, & Kuskov, 2018)

Several key events can be identified that signified a major change in either technology, devices, or cybersecurity. Demonstrating the length of time that cybersecurity has been a known issue in automation and industrial systems (SCADA), one such unconfirmed event is the infection of a Siberian Gas line control system with malware that resulted in an explosion. This event was speculated to be a part of counterintelligence operations undertaken by the Central Intelligence Agency (CIA) during the Cold War, as referred to in a document known as the *Farewell Dossier* (Weiss, 2008). Whilst the truth of the matter may be debated, the application of state agencies to the detection of digital-based threats was identified at least this far back history – signifying that this problem of digital threats to critical infrastructure and industrial control systems is not a new problem.

Whilst the period from 1980-2000 was relatively quiet, there were several smaller incidents within that timeframe, notably an insider attack against the Sewage Treatment Plant in Australia (Abrams, 2008), along with the initial coining of the term "Internet of Things" (Ashton, 1999).

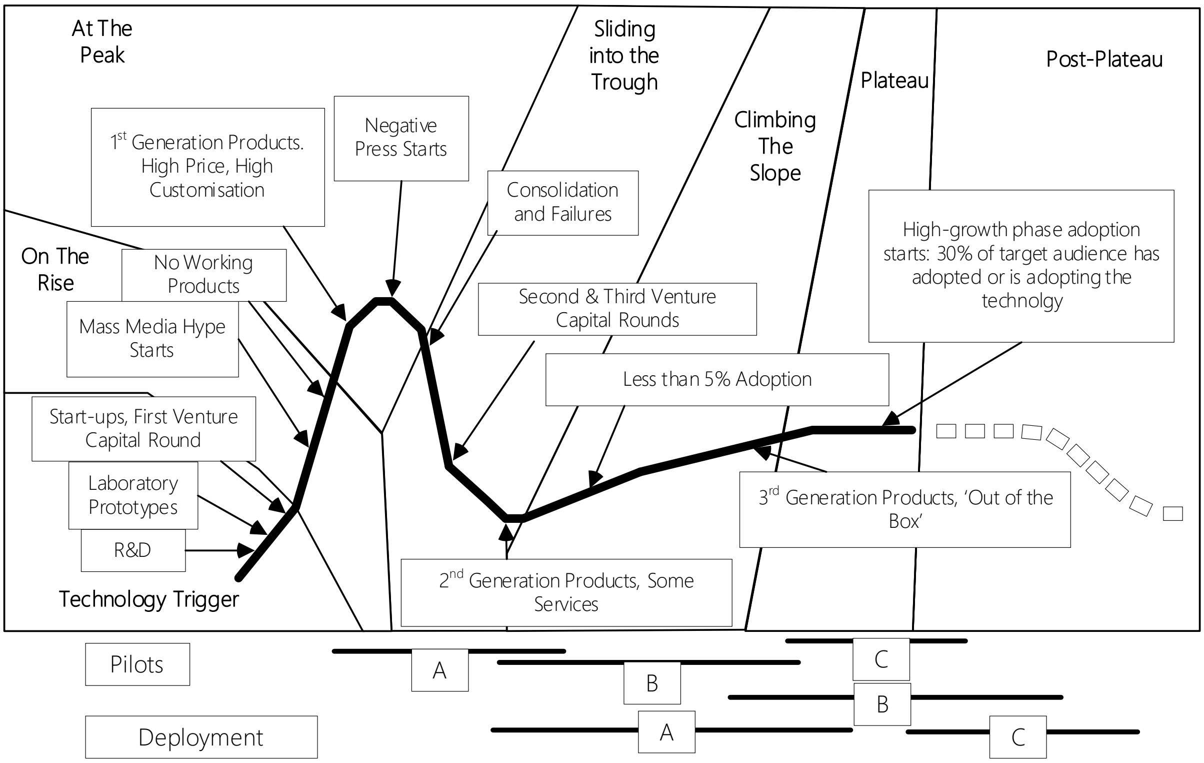
An uptick in noteworthy events occurred from 2000 to 2010 – and perhaps the most well-known infection, "Stuxnet" (Farwell & Rohozinski, 2011). In 2005 the first report on IoT from the International Telecommunications Union (ITU: The Internet of Things, 2005) was published, exploring the usage and future of IoT – including some of the potential devices and applications.

The potential severity and impact of reported cybersecurity events have risen with the increased forbearance of digital connectivity. This is partially driven by new technologies that enable new ways to solve problems and gather data. As an example, IPv6 enables 2^{128} unique addresses, as opposed the ageing IPv4 which only supports 2^{32}. This increase in connectivity allows for an order of magnitude more devices to be connected to networking – correlating to an increased attack surface. This only expands as the value of the data and actions these devices control or can have access to increases.

2.4.2 Marketing and Consumer Expectations

Modern marketing and consumer demands are one of the factors driving IoT adoption. People generally like to have things that make their life easier, and the adoption of IoT to perform smaller, menial tasks fulfils part of this need. An example of this drive for convenience has seen the wide adoption of Smart Speakers in the home from major companies – Amazons Alexa and Google Home as notable examples; however, virtual assistants are also mainstream – Apple Siri, Samsung Bixby, and the Google Assistant. This adoption of IoT based technologies in a known product has normalised adoption and lowered the barriers to usage and adoption for non-technical people. This is coupled with marketing on both alternate and traditional platforms to generate a measured and understood phenomena – hype.

Disseminated by Gartner Inc. (Steinert & Leifer, 2010), the hype cycle can be used to gain a general overview of how products and technologies gain popularity. It consists of seven stages, from technological trigger to normalisation (post-plateau) (Figure 5). This cycle can be seen broadly in most aspects of information technology, in both hardware and software. In recent history, this can be seen in the innovative leaps that came from Silicon Valley in the USA. Each new wave of development was led by a new technological trigger or innovation (Henton & Held, 2013).



At The Peak
Sliding into the Trough
Climbing The Slope
Plateau
Post-Plateau
On The Rise
Technology Trigger
1st Generation Products. High Price, High Customisation
Negative Press Starts
Consolidation and Failures
No Working Products
Mass Media Hype Starts
Second & Third Venture Capital Rounds
Less than 5% Adoption
High-growth phase adoption starts: 30% of target audience has adopted or is adopting the technolgy
Start-ups, First Venture Capital Round
Laboratory Prototypes
R&D
3rd Generation Products, 'Out of the Box'
2nd Generation Products, Some Services
Pilots
Deployment
A
B
C
B
A
C

Figure 5: Hype Cycle, Adapted from (Steinert & Leifer, 2010)

The hype cycle is not without its detractions, namely its lack of scientific basis, the lack of a continual cycle, and subjective terminology (e.g., disillusionment and enlightenment). However, it does function as a rough explanation for the stages present for technological exposure and subsequent adoption.

Despite these misgivings, hype and the subsequent expectations for a given product are a large part of modern technology business. With consumerism as a strong influence, the push for companies to create a better version of their products each year can drive technological innovation, lest they lose the hype and thus, drive for consumers to purchase their products. Whilst the overall issue is far more complicated, as the analysis of hype and its interactions is a diverse and complicated topic – the focus must be on the impact and effects of the phenomena, not the mechanics of its occurrence (Dedehayir & Steinert, 2016; O'Leary, 2008; Steinert & Leifer, 2010).

This push to market new and improved devices, combined with the rapid development and scale of deployment is not possible without a sacrifice being made somewhere in the development process. This sacrifice is usually the security or testing of the product, as this is less obvious to consumers and usually only visible to the internal development and testing team – barring the exposure of major flaws or publicised issues (A. W. Khan et al., 2022).

With similarities to the hype cycle, the backlash when devices do not live up to expectations can be massively damaging to a business's reputation. This can be related to the colloquial idiom of *getting your money's worth*. An example of this is Samsung's Note7 battery issues (Kasprzak, 2017, p. 7) and the IPhone6X Bend-Gate (Kandhari, 2014) issues, which brought much negative attention to companies despite their attempts to mitigate the negative attention. Whilst both examples are from the smartphone industry, IoT shares many of the technologies, owing to the partially shared characteristics, like resource constraints. This sharing of technology presents wide-reaching effects as issues from one company can spill over to another, as core components may share vulnerabilities across a wide range of devices.

Another important aspect is the presence of general social factors, such as a rising view of environmentally friendly and sustainable practices, means that devices that are lower in power consumption and companies with a lower environmental footprint are seen in a more favourable light. Whilst this is not a universal truth, multiple international standards exist to verify sustainable environment practices for companies (International Organization for Standardization, 2019) as e-waste is rising concern and many industries are legislated by governments to adhere to a minimum level of sound environmental practice (Patil & Ramakrishna, 2020).

Implicit trust by consumers (be they businesses or individuals) is built on the predication of a certain level of quality that can be implied from certification against a standard. This can be attributed to the international, collaborative effort of professionals to create the standards and the comparative conditional knowledge of standards in consumers.

This implicit trust can be subconscious or inform conscious decisions (Flavián & Guinalíu, 2006; Michler et al., 2020). Not all consumers will actively check for certifications or standards due to knowledge or other reasons. This trust can be as abstracted from a specific International Standard or certification and instead explained as known or expected functionality. For example, the 802.11 series of standards governing Wi-Fi – the average consumer knows what Wi-Fi does at a conceptual level, and the symbol that denotes Wi-Fi. This comes with a level of expectation that it will work in a certain way and present certain common expected functionality – and work with other devices with the same certification.

This implicit consumer trust is not as applicable for corporations or businesses. As business and corporations exist within the industry, implicit trust can be a starting point, but explicit trust is usually required – i.e., proof of certification. International Standards are written with industry and context experts and agreed on by consensus of all parties and countries involved and can be very difficult to understand and interpret for those not in the industry. As with implicit trust for a consumer, there are International Standards that a business will expect similar organizations to conform to. For example – the risk management standard series for Information Management Systems, contained in the 27000 series of International Standards (International Organization for Standardization / International Electrotechnical Commission, 2013), is well expected for a corporation to conform to. Most International Standards are of minimal relevance to the end-user, as the benefits the standard presents as explicit proof of trust is targeted at wholesale or other businesses – as end-user is not the target audience, nor are they across the technical details of a standard.

This consumer knowledge of standards can drive social expectations, as the lack of meeting this societal expectation can negatively impact the hype around a product, just as severely as negative press relations or scandals can. The following adoption or damnation of a specific technology or device with the current climate of eco-friendly, low impact, high-efficiency devices being pushed to the forefront.

This mix of factors can be summarised as social expectations driving the manufacturing market, with societal expectations of the manufacturing output evolving over time. This is reflected within the International Standards, as they are driven by people in the with experience in the field they are participating in. It must be noted that there is a disconnect between the evolution of best practice and standards, and their associated timeframe of development – standards have long, half-decade review times with best practise often mutating much faster as new knowledge comes to light. This extended lead time creates difficulty in applying cybersecurity protections to IoT, as the ecosystem's rapid evolution operates on a much shorter timeframe – hampering the application of the comparatively slower moving standardisation efforts.

These factors culminate in a dynamic, transforming field, with new technologies created, tested, and summarily adopted, then discarded rapidly by consumers – this creates a challenge with the research, as the target for analysis is in perpetual motion.

2.4.3 Adoption

IoT is already implemented and in use, with Intel's report signifying a ~40% adoption rate in Manufacturing, ~30% adoption in Healthcare, ~8% adoption in Retail and ~7% adoption in Security (Internet of Things (IoT), 2017). This is mirrored in a study by Price Waterhouse Coopers (PwC), who performed a survey of US-Based IoT manufacturers, ascertaining that 38% now offer IoT based solutions, 47% currently offer a solution that incorporates IoT in some form, and that surveyed companies expected to have IoT drive a 10% increase in revenue (PwC, 2017).

Whilst the deployment differs from company to company, they are all shaped by the implementation of cloud-based technologies. Given this extensive adoption and large market expenditure on rapid research, development, and deployment (*Internet of Things (IoT) Market (2021-26) | Industry Size, Growth, Trends*, 2020), with new devices coming to both home and enterprise, IoT is already somewhat embedded into everyday life.

This embedding of IoT devices into daily life acclimatises consumers to IoT. This acclimatisation helps normalise smart device usage and furthers the demand for new applications of the same idea or type of device. New devices, potentially utilising new technologies or repurposing old ones, are subsequently developed and marketed.

With this increased application and interconnectivity, cybersecurity becomes more complex for each network or device type that is connected and implemented. When everything talks to everything else, it is difficult to define where the boundaries of a network lie. This ability to 'boundary box' a network into clear segments (be they physical, logical or a combination of the two) is one of the cornerstones of traditional cybersecurity (Mhaskar et al., 2021). The suite of traditional cybersecurity techniques relies heavily on network segmentation and the availability of computing power to apply computationally expensive protections (He et al., 2017).

This traditional cybersecurity begins to show weakness with blurred borders and outright fails without any borders. This shift also requires a changing in how cybersecurity is approached, as the bounding boxes that are heavily relied on are now blurred or absent.

Some of the technologies at the forefront of IoT are brand new, and this is not always beneficial for dealing with cybersecurity. Corporate IT and traditional risk assessment do not always handle new, relatively untested technologies, as assessment frameworks or techniques may not know how to accurately assess the new IoT based devices (Nurse et al., 2017). In a risk-averse ecosystem for larger corporations, this leads to slower uptake of newer technologies. The inverse can also be true – newer, smaller companies will try the new technologies to get a competitive edge, adopting the bleeding edge of technologies and innovations.

Large corporations are averse to sweeping changes and move comparably slowly compared to small start-ups in knowledge and application of new technologies. Smaller companies are more agile and do not have the size and bureaucracy hampering the rapid deployment and testing of new ideas (Dedehayir & Steinert, 2016; O'Leary, 2008). The ability to cut and run on something not working as imagined is much easier for a small company, where the overall effort required is smaller. This rapid adoption and discard cycle is a major driving factor for the evolution of the IoT ecosystem, directly impacting the difficulty in applying cybersecurity protections to such rapidly evolving and diverse applications of IoT.

2.4.4 Ethics and Data Protection Legislation

With the advent of big data, regulation and oversight have steadily attempted to keep abreast of the rapid and dynamic change within the technology industry. Whilst 'Big Data' has beena driving factor for regulation, the further exploration of 'Big Data' is not in scope. Regulatory bodies have started to tackle the digital challenges, with the introduction of Software as a Medical Device (SaMD), particularly shaking up the older regulator process, as it was outside the traditional scoping for medical devices. These regulations have been rapidly changing, with each country tackling it in their own way. The United States of America (USA) has the Health Insurance Portability and Accountability Act (HIPAA), the European Union (EU) has the General Data Protection Regulation (GDPR) and Australia has Australian Privacy Principles (APP). Each regulation focuses on privacy but has differing scopes of applicability, regulator reach and cooperation across international borders.

This rapid change also includes a focus on the application of these devices to healthcare and health. The subsequently created Governmental agencies and departments have expanded horizons to tackle this new problem – in the USA, the Federal Trade Commission (FTC) released a report on this issue – urging uptake of best practice and an overview of the extensive potential security and privacy risks (Internet of Things: Privacy & Security in a Connected World, 2015). The FTC also has an investigative mandate to ensure compliance and verify breaches of HIPAA legislation. The GDPR is enforced by nominated 'Supervisory Authorities' (SA), who have their own set of requirements under the GDPR (each member state is required to nominate at least one SA) and is usually the existing privacy agency, for example the UK's Information Commissioners Office (ICO).

The EU's General Data Protection Regulation (GDPR) (The EU General Data Protection Regulation (GDPR), 2017) provides some history on the harmonisation of data privacy among the European Union Member-States and the subsequent request for a coherent and universal set of legislation to target data privacy. This outlook and request for a universal set of legislation culminated in the creation of the GDPR. The GDPR presented new additions for how data around a persons' actions online were to be managed – their 'digital life', a first for legislation of this type. This first step into digital information management involves the right to be forgotten and the right to request all personal data held. This change necessitated a corresponding addition or modification to any system that stored the data identified in the legislation to ensure adherence to the mandated functionality.

The Australian Privacy Principles (APP) list 13 specific principles that guide an organisation when dealing with personal information. This personal information is defined as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable. These principles govern the handling of personally identifiable data and can be a concern when implementing IoT based tracking or analysis measures. In general, these can be categorised into:

- Unauthorised surveillance
- Un-controlled data generation
- Un-controlled data use
- Inadequate authentication
- Increased information security risk

Australia has also passed the '"Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018" (AA Act / AA Bill), which has been lambasted on the world stage – due to the potential for secret (cybersecurity) weakening of systems - and associated quote from Former Prime Minister Malcolm Turnbull "the laws of mathematics are very commendable, but the only law that applies in Australia is the law of Australia", (Crozier, 2019) and discussed internal to the country as to its effectiveness and usefulness as a whole (Article | The Assistance and Access Act, 2019). Given the wide-reaching aspects of the bill, IoT devices and communications can fall under its purview and must thus it must be acknowledged as a potential source of problems.

Commonly known as the 'Privacy Rule' and the 'Security Rule' the USA Department of Health & Human Services has created a condensed subsection of the HIPAA regulations to better disseminate the critical information to the complicated area of cybersecurity and compliance. HIPAA has a relation to the Health Information Technology for Economic and Clinical Health Act (HITECH) - HITECH strengthens and informs part of the HIPAA regulations. These regulations are complex and have spawned a section of the market that tailors consulting for just HIPAA compliance services and a plethora of checklists and overviews are available (*HIPAA: Security Checklist*, 2019; Klein & Monson, 2015).

2.5 IoT Cybersecurity

Cybersecurity is now a key component of modern communication across a wide range of users and consumers – from billion-dollar corporations to a layperson browsing the Internet. This wide range of users understand at differing levels that cybersecurity is essential; however, the application of cybersecurity protections is still not always maintained to the level of rigour expected, even with this understanding of its importance. As such, the cost of cybersecurity incidents is rising, with new technologies creating more issues (especially in IoT), and this being corroborated by multiple reports (*Cyber Security Breaches Survey 2018: Statistical Release*, 2018; Romanosky, 2016; Tuttle, 2022), creating a greater demand for cybersecurity.

This need for cybersecurity across all aspects of technology is continually playing the 'catchup game' as new technologies, platforms, and techniques for exploitation are developed faster than cybersecurity techniques can be adapted to contain them. This catchup is evident in the emergent IoT technologies, where cybersecurity techniques that are tried, tested, and true have formed the foundation of how we secure non IoT systems, no longer providing adequate protection.

The following sections will discuss this further, expanding on problematic concepts in IoT and some of the issues with current cybersecurity practices - including defence in depth, the different common attack vectors, and physical security. This framing of common broad cybersecurity practice then enables further discussion issues in current cybersecurity frameworks for IoT.

2.5.1 Problematic Concepts in IoT Cybersecurity

Traditional cybersecurity techniques is another term for the current understanding and approaches to the application of cybersecurity for non IoT systems (Souppaya & Scarfone, 2012; Wilamowski et al., 2017). These techniques include (but are not limited to) the application of logical separations, defence-in-depth, and the multitude of frameworks based around fundamental principles of cybersecurity; culminating in an extensive body of knowledge that has been continually updated, upgraded, and modified for decades.

These fundamental principles and approaches have not been rendered irrelevant by IoT – the core principles and approaches are still applicable to cybersecurity in IoT and non IoT networks. However, there is a shortfall – the existing techniques are poorly equipped to handle significant changes in layout or scope. As a result of the change to both the layout and scope of networks, the existing frameworks have bent, and in some cases, broken. Creating a new framework that considers new networking technologies, the increased connectivity (between both people and devices) and builds on the strengths of the lessons learnt from the traditional principles of cybersecurity is required to compensate for the extensive changes that have occurred with the implementation of IoT.

2.5.1.1 *Defence in Depth*

Defence in depth is one of the core tenants of cybersecurity, which is defined by the National Institute of Technology (NIST) as "Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization." (Souppaya & Scarfone, 2012). The base principle is that the more layers of different defences that are employed in cybersecurity applications, the more chance there is of detecting, responding to or preventing an incident. This principle still applies within the newer, IoT-based networks. However, it does need special consideration for the types of devices – as an example, a device level firewall is not always feasible for IoT devices, particularly low-powered devices due to the inherent computing constraints.

The pillars of cybersecurity, or more aptly named guiding principles are *Confidentiality, Integrity, and Authentication*. Sometimes called the triad or the CIA triangle, it is commonly extended to include *Authorization* and *Accounting* and *Auditing*, (Wilamowski et al., 2017) forming the combination of CIA and AAA (Soltys, 2020). These principles form the cornerstones of all cybersecurity approaches and guide the application of cybersecurity measures of all types - the application of these principles result in two main approaches when dealing with *Authorization* and *Authentication*. This principle of least access states that using a given system should have only the amount of access they need to complete their job and no more. For example, users generally should not have direct access to the backend database unless it is essential to complete their job activities. In practice this takes many forms – an example of which is Role-Based Access Control (RBAC), like Microsoft Active Directory and subsequent application of group policies allow for fine-grained control of users' ability to perform actions on a windows desktop - as these access control schemas are generally centralised, and can take significant computing power as the number of rulesets increases. This heavy computation is an issue at the 'end of a networking' where IoT devices resides, as these devices are not guaranteed to have the computing power needed to handle such a heavy and detailed access control system.

2.5.1.2 *Attack Types*

The different types of attack facing IoT networks encompasses the existing threats know to cybersecurity, with malware taking the forefront. Malware describes all types of malicious software; malware has expanded as computing has become more powerful – the advent of crypto-lockers is a (relatively) new threat that malware protections must deal with. Existing protection all focus on scanning of some type, be it passive or active and are usually signature-based. As such, these are not suitable for devices that run in low-power mode – the power and processing requirements are too high to allow the device to function for an extended period without intervention. The possible attack types are numerous, however only the recurrent themes from the literature are discussed here – this also includes the limited inclusion of the results of compromises, like a Distributed Denial of Service attack using compromised IoT devices (Vlajic & Zhou, 2018; Wang et al., 2017).

Networking technologies have evolved to become faster and denser, targeting both throughput and volume of connections. With the application of new ultra-low-power network protocols, the trade-off between features and security is still a constant issue. As such, newer network protocols attempt to integrate security into the protocol (Russell & Duren, 2016); however, advanced security processing is not always possible when working with the target devices. Thus, the support for these network protocols is not always present on devices.

These protocols are also an issue for intrusion detection/prevention systems (IDS/IPS) that require active scanning or monitoring of either network traffic or associated logs (or both). As these IDS/IPS rely on many differing detention mechanisms (signature, pattern, and event) to detect intrusions, new protocols require time to be fully understood by these systems (Igure et al., 2006). IDS/IPS can take active action against detected intrusions or notify administrators of an adverse event. This type of active scanning and analysis is not suitable to low powered devices, given the high degree of processing and analysis required. These systems are also usually located on core network paths or checkpoints and can require dedicated specialised hardware.

Converging networks describe the conglomeration of different devices and networks into a shared resource space. This convergence has been aided by the ease of interoperability and standardisation of protocols. Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Internet Protocol (IP) have greatly aided interoperability by creating a shared networking stack (Harris & Hunt, 1999). This joint communication base has allowed disparate devices to share networking space more straightforwardly, combined with logical networking technologies like Virtual Local Area Networks (VLAN's). However, this was not the driving factor that pushed the convergence of networks– cost cutting and the creation of more complicated systems of systems that need digital communication fed into this cycle.

2.5.1.3 *Physical Security*

Physical security is an essential factor for cybersecurity protections, with IoT creating specific challenges for physical security. The distributed nature of IoT devices, coupled with their small size and the overall numbers of devices that can potentially be deployed, creates a lower bar for physical security problems (Yilin Mo et al., 2012). As IoT devices cannot by nature be secreted away in a secure room behind chase-gates or RFID card access doors in patrolled areas, without defeating their intended purpose, tracking, and managing the access to these devices is a formidable task (Kobara, 2016). As IoT devices are (generally) connected to a network that has internal access to, the numerous, small-scale devices substantially expand the potential attack surface and create a potential entry point for the beginning of a larger incident. This increased attack surface is due to the placement of IoT devices – the devices are human accessible and as close as possible the needed measurement location – rarely do such locations coincide with secured areas, unlike traditional infrastructure (Kobara, 2016).

2.5.2 Shortfall in IoT Security Frameworks

IoT creates a new aspect of cybersecurity that is not easily captured by existing frameworks and tools. Many of the traditional techniques used rely on chokepoints and layers of security in a high controlled manner – this is not always possible with IoT networks, given their unique characteristics. The following section will examine existing frameworks for IoT cybersecurity and the major contributing factors to the ability to apply cybersecurity protections to IoT using the existing IoT cybersecurity frameworks – integration, new technologies, compute restrictions, and network boundaries.

2.5.2.1 *Existing Frameworks*

There are existing frameworks for IoT cybersecurity and best practise, put forward by parties ranging from conglomerates of networking professionals (GSM Association / GSMA), companies with their own IoT platform offerings (Microsoft), to cybersecurity focused technical groups like Open Web Application Security Project (OWASP) to governmental agencies like the National Institute of Standards and Technology (NIST) and European Union Agency for Cybersecurity (ENISA).

These reports and guidelines vary in detail, completeness, and overall usefulness to the application of cybersecurity. For example, the NIST IoT Report (Greer et al., 2019) focuses on the classification and analysis of the current ecosystem language. While not a set of direct actions, it is valuable to understand some of the nuances of the scattered terminology of the IoT ecosystem – including interrelations between IoT outlooks (refer to Section 2.2) and relation to other computing areas.

In the same vein, the G4 Report (Schrecker et al., 2016) in IoT cybersecurity and risk is lengthy, informative, and highly detailed regarding potential threats posed to the IoT ecosystem. This report details some general terms and makes several pointed reminders of the unique aspects of IoT that must be acknowledged – physical security and physical risk are among these. As an industry report, it draws heavily from existing standards and frameworks published by standards and national bodies. It also refers to applicable methodologies like Spoofing, Tampering, Repudiation, Denial of Service and Elevation of Privilege (STRIDE). It makes it clear that cybersecurity of IoT is not just an end-user problem, it must be tackled at all levels – from the design of devices to deployment and ongoing maintenance. This is partially mirrored in the series of documents by the GSM Association, focussing on backhaul providers and covers all aspects of deployment of the associated infrastructure and required security provisos (*IoT Security Guidelines Overview Document V2.0*, 2017; *IoT Security Guidelines for IoT Service Ecosystem V2.0*, 2017; *IoT Security Guidelines Endpoint Ecosystem V2.0*, 2017; *IoT Security Guidelines for Network Operators V2.0*, 2017).

National organisations are also producing guidelines for IoT, with the Internet of Things Alliance Australia (IoTAA) outlining basic guidelines for those unfamiliar with IoT (*IoTAA: IoT Security Guidelines*, 2017). These guidelines detail the need for forward planning – disruptive technologies like 5G and subsequent network topology changes that 5G allow, need to be accounted and planned for at all levels – from networking to device support, and must include all devices, not just IoT.

The European Union Agency for Network and Information Security has also produced an IoT security framework (Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures, 2017), which, similar to NIST, describes the minimum expected protections that must be deployed for IoT (and other) networks.

The Internet of Things Security Foundation (IoTSF) have also published a Security Compliance Framework (*IoT Security Compliance Framework*, 2016). This document is published but notes that it is currently unfinished and still in development. What exists of the document presents a foundational framework for IoT cybersecurity based on existing cybersecurity principles. Other organisations, both national and international, are putting forward security guidelines that govern over their own area of concern (*Embedded Hardware Security for IoT Applications*, 2016; *Internet of Things (IoT) Security and Privacy Recommendations*, 2016a).

Companies that produce or consume IoT in some fashion also produce their own IoT security frameworks. The Open Worldwide Application Security Project (OWASP) is a community-driven project that contains multiple documents and is a source of additional information. Within the OWASP document collection is a primer for selecting and assessing a potential IoT security framework (IoT Framework Assessment - OWASP, 2016). Microsoft, who offers a cloud platform that allows the integration of IoT devices, also put forwards a more informal document of IoT best practise in general (Internet of Things (IoT) Security Best Practices | Microsoft Docs, 2018).

Overall, these documents vary in focus, detail, and informational quality. Many cover the same core cybersecurity principles; however, there are many more documents published globally, each document containing its own view of IoT and its layout. This narrow focus on industry specific IoT deployments can be related to the fragmented IoT ecosystem, both in the language of the ecosystem and the devices in their application and focus.

2.5.2.2 *Integration into Existing Infrastructure*

Integration of IoT into existing networks comes with new challenges. Not all IoT devices can utilise Wi-Fi's standard (IEEE 802.11 Series) for wireless communication. Instead, they may use Zigbee, 6LowPAN and other protocols that are not out of the box compatible with the existing infrastructure. This difference in protocols creates a point of integration, that, when done poorly, can create ad-hoc, patched-in networking that is not as secure as a redesigned network. These potentially poor integration points create additional points for exploitation.

Network layouts have changed to take advantage of the benefits provided by internet connectivity. Cloud-based layouts are varied, widespread and have a low barrier to entry. This ease of use and availability has driven a shift in businesses approach to networking, with cloud integrated systems now becoming the default approach (Shuaib et al., 2019). The usage of Cloud approaches also lends itself to the usage of BYOD as a means of lowering capital infrastructure costs.

BYOD cybersecurity is a trade-off between greater user control and less institutional control. BYOD devices are generally untrusted and approached using the Zero-Trust Model – assuming that all devices are untrustworthy by default (Kindervag & Balaouras, 2010). Given that BYOD devices are now dual usage devices, with both work data and personal data existing side-by side on the same physical device, the potential for IoT devices to amplify a cybersecurity incident is significant. As IoT devices are more widely adopted, the link between BYOD and IoT becomes another area where the existing techniques and knowledge was not written to account for IoT, and thus falls short. Care must be taken to not treat IoT as an extension of BYOD, as while they are similar and can benefit from each other, they are distinct enough that approaches will need to be tailored to account for the characteristics of the devices.

With the proliferation of BYOD and the overall increase in awareness of cybersecurity, users are likely to keep abreast of training, and other cybersecurity measures to protect an individual from targeted attacks (Palanisamy et al., 2021). At the same time, users are more likely to question what their devices are being used for, and more aggressive protections like active usage monitoring and remote lockouts are less likely to be accepted on personal devices (Martin, 2014).

2.5.2.3 *New Technologies*

New, and therefore immature technology suffers from the inherent issues of first-generation products. In cybersecurity, the maturity of the platform, technology, and protocols play a large factor in the comprehensive analysis of the device, its usage, and its potential impact on a network. IoT is a relatively new device type, the associated platforms are new, and the protocols are either repurposed, expanded, or new (Rani & Gill, 2019). The overall maturity of IoT as a platform is inferior to cloud services. While the new platforms build on the existing platforms to obtain a 'jump-start', this jump-start does not help with the core cybersecurity of the devices.

Most of the IoT devices present in the marketplace and deployments are first or second-generation devices. These devices are usually highly dependent on specific deployment criteria, are not highly interoperable with other devices, and are unlikely to be moved from where they are first deployed. This is contrary to a core IoT vision, where devices are ubiquitous and plug and play between networks (and devices) freely (Borgia, 2014). This high overhead, coupled with the specificity of deployment and purpose, means that security, deployment layout and design can fall into the 'too hard basket' and be done poorly. This ease of deployment and security by default will come as the IoT ecosystem matures.

2.5.2.4 *Low Powered Devices*

IoT devices are usually small enough to be powered by a battery for extended periods, anywhere from weeks to years of total operational time. This operational window creates two immediate issues – that these devices are small, scattered across a vast area, and that the devices may not always be active on a network.

This low-powered nature precludes the device from some of the traditional aspects that require a comparatively large amount of processing power to perform, such as Public/Private key verification and Transport Layer Security (TLS). There is no technical barrier to implementing these protections, however they are generally not operationally feasible to be added to many of these ultra-low-powered devices (Boeckl et al., 2019). The overhead of the cryptographic operations would exceed that of the device's ability to compute or reduce the operational time dramatically.

2.5.2.5 *Management and Updates*

Updating and managing IoT devices is yet another area that traditional techniques may fall short in addressing IoT. IoT devices are not always online and may be as small as embedded microcontrollers with specific updates. The challenge is how to update, maintain, and effectively secure IoT devices when the feasibility of Over-The-Air (OTA) updates are not guaranteed to be technically or operationally feasible (Boeckl et al., 2019).

The need for cross-domain and discipline knowledge has always been an issue in cybersecurity. The wide breadth of knowledge required for effective protections creates the potential for inadvertent deployment of incomplete protections, due to a lack of knowledge (Borgia, 2014). This specialist knowledge requirement is compounded within IoT – an entirely new, different, and challenging area of knowledge that essentially throws out the old rules and techniques of cybersecurity and replaces them with something that is, at this point, not yet known. The traditional cybersecurity frameworks and body of knowledge are only partially applicable in this new area of security and computing. With the rapid expansion and adaptation of devices and applications to new and existing areas has created an ecosystem where cybersecurity is lagging behind the implementation (Khan & Salah, 2018) - lacking the tools and knowledge to support the application of cybersecurity.

2.5.2.6 *Network Boundaries*

As networks are now more interconnected, the traditional bounding boxes of physical and wireless segregation are becoming rarer. Logical networks can now incorporate remote, cloud and virtualised assets (Bull et al., 2016). This extension networking outside of physical assets is magnified by IoT, creating the potential for ever expanding networks that have ever decreasing clarity of where one network begins and another ends.

2.6 PROBLEMS IN IOT

The IoT ecosystem can be described as the amalgamation of smart devices, different computing paradigms, consumer needs and new technologies that facilitate new approaches to existing or future problems. This ecosystem of novel devices and approaches create an area where cybersecurity protections face issues as diverse as the ecosystem.

Dependent on the architecture employed, the security analysis and controls employed will differ. Whilst this research is not concerned with the process and performance of security analysis; it does seek to inform them. As such, the differences for each of the deployment architectures will need to be accounted for. When assessing risk, the core goal of cybersecurity is to identify the potential threats and their subsequent potential impact against an organisation.

With data regulations becoming a significant factor in data governance, the need for clearly defined protections and internal policy to help protect companies against cybersecurity incidents is clear. The application of protections is made more difficult by the integration of IoT, expanding the potential avenues of attack ("Master IoT Cyber-Security Challenges with Comprehensive, Multi-Layer Security," 2019).

The current issues with IoT architecture are multifaceted and numerous. The lack of unified linguistic definitions of IoT presents an issue, but it is not the sole problem. As with all new technologies, the ecosystem surrounding it has not stabilised nor has it gained the expected maturity. As such, a lack of unified architecture, tailored solutions, and standalone implementations, with little to no cybersecurity, or privacy concern, regulatory oversight, data handling and consideration of convergency of systems, are all facets of the multidimensional problem.

2.6.1 Issues in HIoT

HIoT inherits the issues from IoT and expands on them due to the unique challenges of healthcare networks. Regulatory oversight is more imperative in conjunction with legal and ethical concerns. These areas, such as privacy regulations (which differ by jurisdictional area), create difficulty in developing and integrating new technologies (Australian Government, 2014; Council of the European Union, 2016; Health Information Privacy, 2015). This difficulty results in a specific, vertical fit for singular purpose deployment of HIoT technologies and does not lend itself to interoperability and IoT's goal of ubiquitous computing. This type of deployment is comparable to the previous generation of medical devices – standalone, isolated, or proprietary medical devices that were not designed for broad interoperability within a system of systems (S. Campbell, 2010; Tarouco et al., 2012).

Older devices are still in use, as the previous generation of medical devices have extended lifetimes, and some devices cannot be easily replaced – for example, a Magnetic Resonance

Imaging (MRI) machine. As such, these legacy devices are prevalent on the network and are unable to be upgraded or physically moved in many cases. These devices exacerbate the issue presented by HIoT, as the expanded attack surface allows for a greater risk associated with the connection of these devices (Williams & McCauley, 2016). This combination of factors generates discussion of security and privacy around how devices dealing with sensitive healthcare and associated personal data can be secured.

Newer IoT and remote medical based applications inherit the broad applicability of IoT to create a diverse portfolio of potential uses in both clinical and non-clinical applications. As the application of HIoT opens the doors to myriad applications and sensor data, the created and theorised system range from all-encompassing, 24/7 embedded and ambient patient monitoring systems (Vlamos, 2017), to embedded wireless cardiovascular monitoring to detect a heart-attack, using movement tracking to assist in diagnosing disorders such as epilepsy and Parkinson's Disease, enabling fall detection in ages care facilities and enhancing fitness monitoring opportunities (Qadri et al., 2020).

This wide range of applicability creates issues with HIoT on top of the inherited issues present across the IoT ecosystem. as discussed by Haghi Kashani et al. (2021), the current state of research in HIoT covers a diverse range of approaches and focusses – a non-exhaustive list of includes HIoT specific protocols, system architecture, resource management, optimisation, cybersecurity, interoperability, and scalability. This wide range of research exacerbates the issues with IoT and creates issues with terminology.

2.6.2 Issues with Terminology

The language used within and to describe IoT (and its subsets) inherits the fragmented nature of the devices and the ecosystem. This creates an issue where language has not yet stabilised, with many slightly different terms referring to identical concepts within the same ecosystem. While this is not a new problem – every multidisciplinary field must deal with the overlap between acronyms and terminology due to converging fields, the rapid research and development of IoT has exacerbated this phenomenon.

This creates multiple issues related to both research and understanding. New keywords appear with regularity creating difficulty in scoping, causing further analysis to identify any overlap between old and new terminology and where it (the new term) relates back to the core concept.

This core concept may not be readily apparent from the terminology used, as IoT has multiple viewpoints on what it is and how it should operate. Some headway has been made to tackle this problem, with The National Institute of Standards and Technology (NIST) defining the different ways one can interpret the current in flux terminology as it related to their preferred nomenclature of Cyber-Physical Systems (Greer et al., 2019).

As this issue is a fundamental issue in the identification and definition of IoT, the language terminology is discussed in depth in 4.5.2, Language and Context.

2.6.3 Alternative Approaches

One of the new aspects of cybersecurity is the shift from a device centric view to a data centric view. To sidestep the issues of low computation power of IoT devices, gateways and orchestration devices with more computational power become communication hubs of an IoT network – of which an example is edge computing. These edge computing devices, more in line with traditional servers, have more computational power to examine dataflow and perform operations that determine if a device is sending the correct data or not and if the device should be allowed to communicate with the wider network.

Trust networks and Trust webs may come into play as a valuable and innovative approach to cybersecurity in IoT. While they are not in visible mainstream use yet, the principles of trust webs and frameworks have aided cybersecurity and cryptographic approaches. The Trust Chain of the Public Key Infrastructure (PKI) that enables Secure Socker Layer (SSL) and its replacement Transport Layer Security (TLS) for the World Wide Web, is an example of such an application. IoT will require a unique application of these ideas; however, their potential for solving the issue of applying cryptography in IoT networks must be acknowledged (Durand et al., 2017).

From Table 2, the issues identified are a combination of technology and process. As technology and process are intertwined, it is impossible to solve all issues in one without also solving the issues in the other. This is made more complex when IoT devices are included in any potential solution, as the IoT devices present a new and variable aspect to any system due to current flux in the IoT ecosystem.

Part of the solution is maturity of technology and platforms, as it is near impossible to have technology of process account for all aspects of a given domain, especially when that domain is under rapid evolution. Given time, the IoT Ecosystem will 'Calm Down', allowing processes and technologies to stabilise. This stabilisation will also give the currently incomplete understanding of cybersecurity in IoT the needed foundation to build reach maturity.

Cybersecurity is a complex and multifaceted problem, and the lack of maturity and rapid development of a platform makes it exponentially harder – cross domain, cross platform, and integration of IoT into existing systems creates a messy and complex area where multiple solutions exist to solve any given cybersecurity issue. The first solutions will almost certainly be flawed, and multiple iterations of refinement and improvement will be required – which, without a stable base from which to build the understanding, will ultimately result in a even greater flaws in any given solution.

2.6.4 Ecosystem Wide Issues

The key issues identified within the ecosystem cover a broad range of subject areas, disciplines, and root causes, similar to the IoT ecosystem itself. Table 2 presents a summary of the issues identified from the literature. This is discussed in more detail in the following chapter.

Table 2: Summary of Issues Identified form the Literature

Issue	Overview	Impact
Lack of coherent descriptive terminology (Section 2.6.2)	IoT has many differing terms for similar or identical areas of the ecosystem	Information is harder to find; the overall knowledge base becomes fractured
Lack of coherent ecosystem (Section 2.6.3)	Providers of IoT are per-device or per-platform, with little to no interconnect	IoT deployment are vertical instead of horizontal in nature
Application of current cybersecurity techniques subpar (Section 2.5)	Traditional cybersecurity techniques fall short in effectiveness when applied to IoT due to the nature of devices	Poor cybersecurity across all aspects of IoT
Devices are radically different (Section 2.3.3)	Devices are developed independently, and for a purpose (mostly) as such, they vary greatly in capabilities and design characteristics	Devices can be too different to apply coherent or consistent security techniques
The blurring of Lines between Physical and Digital realms (Section 2.3.1.1-4)	Convergent systems create overlap between digital identity and the physical actions and device	Greater attack surface and the ability for digital actions to have physical impacts
The deployment scale and number	Devices can range from a bare handful to hundreds of thousands of	Managing devices at scale is an existing cybersecurity issue

of devices (Section 2.3.2)	sensors depending on the deployment	
Unique constraints for hardware, software, and networking (Section 2.3.3)	These three aspects of IoT have differing unique constraints per device, usually due to design or performance issues	One solution for IoT security may not fit all devices and must be tailored
New technology, immature in comparison to existing infrastructure (Section 2.5.2)	Traditional cybersecurity has a history of proven techniques that can be applied, whereas IoT does not have this body of knowledge and proof	Lack of knowledge creates unknown unknowns; knowledge gaps in protections applied
Lack of awareness (Section 2.4.2-3, 2.5)	IoT is a new and exciting field, and as such, the awareness of threats and issues around such deployments are not fully understood or appreciated	Awareness and knowledge are of critical design importance, and until awareness is highlighted, it can go unnoticed
Insecure design and development of devices (Section 2.3.3)	The software has known issues when time pressure is applied; these issues are magnified with IoT as the devices have less room for error	Devices have higher constraints leading to greater difficulty in development
Fragmented security approach and regulations (Section 2.5.2)	Regulations and security frameworks are not coherent across the entire ecosystem	Lack of security guidance and framework leaves open holes for cybersecurity flaws
Economic initiatives lacking (Section 2.5.2.1)	Economic initiatives from governmental organisation to develop secure IoT are somewhat lacking	Less focus on economic benefits and initiatives means companies that do implement are looking for the best cost vs. benefit, which usually lacks security
Product Lifecycle management lacking (Section 2)	Lack of coherent full-spectrum device lifetime management framework	Management of IoT devices is completely different in application than other existing techniques

2.7 LITERATURE SUMMARY

The issues facing the IoT ecosystem are not just a technical issue – the overall maturity of devices, process and knowledge are also sources of potential issues. This interconnected nature of the IoT ecosystem means that any one solution cannot be formed in isolation, as the forces and considerations will feed in and out to multiple areas of the IoT ecosystem.

Without the examination and understanding of the IoT ecosystem, and both the technical and non-technical based factors, any solution made to address an issue runs the risk of missing one or more segments. This possibility of oversight when creating any solution for a problem, not through malice, but through the difficulty of understanding and defining such a blended ecosystem. This difficulty is exacerbated by the known limitations of IoT devices rendering some segments of the existing body of cybersecurity knowledge inadequate. Currently there is a lack of understanding of the larger implications of cybersecurity in IoT, what cybersecurity protections and processes can be translated and what cannot be translated and what is missing in the protection of IoT. The tools exist to tackle this problem – although there will not be a single silver-bullet style solution.

As such, any solution must address the identified issues in the literature - tackling the relative immaturity of specialist IoT cybersecurity frameworks, the lack of defined system boundaries, the rapid evolution of the IoT ecosystem – especially the associated effects of this rapid evolution on perspective and the terminology, regulatory and governance issues and the capabilities of the highly variable IoT Devices.

In addition to the issues stated above, the literature has also highlighted the wide range and application of IoT, reaching both consumer and enterprise in applicability, and each with their own set of wants, needs and expectations; yet another influencing factor in the IoT ecosystem that must be accounted for when designing a solution to address any issues identified. As such, this research will focus on addressing the identified shortcomings in the current cybersecurity guidance.

3 METHODOLOGY

Methodology is defined by the Merriam-Webster dictionary as the *"…body of methods, rules, and postulates employed by a discipline: a particular procedure or set of procedures"* ("Methodology", n.d.). This definition adequately describes a methodology in its barest form yet does not cover the depth and breadth of what can exist within a methodology across the research continuum – from Quantitative to Qualitative research paradigms. This means that there are a multitude of conceptual frameworks, methods, approaches, test of rigour, and research designs that are derived from blending the two opposing viewpoints along the continuum of research.

The research continuum is the spectrum from positivism to interpretivism. Given these two opposing paradigms on how a researcher analyses the world to generate knowledge, the differences must be highlighted.

For the positivist paradigm, the underlying belief is that knowledge is generated from repeatable, externally verifiable events (Creswell, 2014). The scientific method of question, test, analysis, and the re-test is grounded in this viewpoint of knowledge generation and is common in the colloquially termed 'harder' sciences – like physics. This observable and reproducible approach opposes the colloquially termed 'softer' sciences, which are concerned with interactions between people (Creswell, 2014). Within an interpretivist outlook, the underlying belief is inverted and becomes the view that knowledge is now subjective, based on one's interpretations and experiences.

This debate on opposing viewpoints has been repeated throughout history. The viewpoint of universal truth, stemming historically from Socrates and Plato; versus the subjective truth from the sophists such as Protagora and Gorgias to the combination of the two, such as Aristotle's Golden Mean or Cicero (Johnson et al., 2007). These two opposing viewpoints can be termed purist. In reality, the two viewpoints collide and draw from one another to form a cohesive whole.

3.1 Conceptual Frameworks

Conceptual frameworks underpin all research, even when not directly articulated (McGaghie et al., 2001). Even if a conceptual framework is not explicitly stated, it is usually trivial to construct at least a brief rationale for any given study (Ravitch, 2017). A conceptual framework will vary in length, complexity, and outlook across and between research fields; they are also dependent partially on the researcher and their outlook on how research and knowledge should be conducted (Creswell, 2014; Rogers, 2016).

This proposition that a conceptual framework is constructed of a researcher's knowledge and view of knowledge generation is insufficient to articulate the complexities and nuances of what a conceptual framework *is*. Ravitch (2017), notes that there are at least four separate ways the literature describes a conceptual framework. A Conceptual Framework can refer to either a visual representation of a study's major theoretical tenants; be treated identically as a Theoretical Framework, dependent on how one defines theory; a way of linking the separate aspects within the research process; an argument as to 'why' one wants to study a given matter and why the prescribed method is appropriate and rigorous.

By combining the third description (the linkage of research elements) and the fourth description (the argument as to the 'why' of the research) we can begin to define the individual components of the conceptual framework. By articulating the individual components and their subsequent interrelations creates the conceptual framework for this research.

This articulation is displayed in Figure 6, which was constructed in the following manner. Firstly, the out bounding box is set to contain the conceptual framework, which is made up of multiple individual aspects (Ravitch, 2017). These individual aspects are discussed in detail in later sections, following the order in Figure 6. The first aspect that drives all further conceptual decisions is the selection of a positioning theory – this theory shapes how researcher looks at all the system(s) under study (Hevner & Chatterjee, 2010). As such, this is the first part of the conceptual framework.

Next, a researcher must be cognizant of their own bias – by explicitly including this research interpretation as a portion of the conceptual framework, bias can be managed (Dube & Pare, 2003). As the researcher is intrinsically linked to the research, this bias management is the second part of the conceptual framework.

Next, reason and rigour can be articulated for a given research project. Reason denotes why the researcher wants to do the research and the potential impacts of the research. Rigour is the articulation that the research is of sound scientific rigour. Both reason and rigour will affect the method selected, as well as the limitations present in any selected approach (Ravitch, 2017; Rogers, 2016).

Next, by taking the positioning theory, researcher interpretations, reason and rigour, a method can be selected that fits the conceptual framework and the research (Yin, 1994). Finally, the limitations of the research as a whole and the method can be articulated (Creswell, 2014).

The aspects of positioning theory and managing researcher interpretations need no further fragmentation, as they can be clearly articulated at this level. Reason and rigour, however, must be split further into their constituent parts.

In this case, reason is described as why the research is undertaken – including both the impact of the research and the reasoning behind the decisions made. Rigour relates to scientific rigour of the research in that the argument is made that the research is rigorous and complete in its approach. As an example, rigor is defined by the National Institute of Health (NIH) as "The strict application of the scientific method to ensure robust and unbiased experimental design, methodology, analysis, interpretation and reporting of results" (National Institutes of Health, 2015).

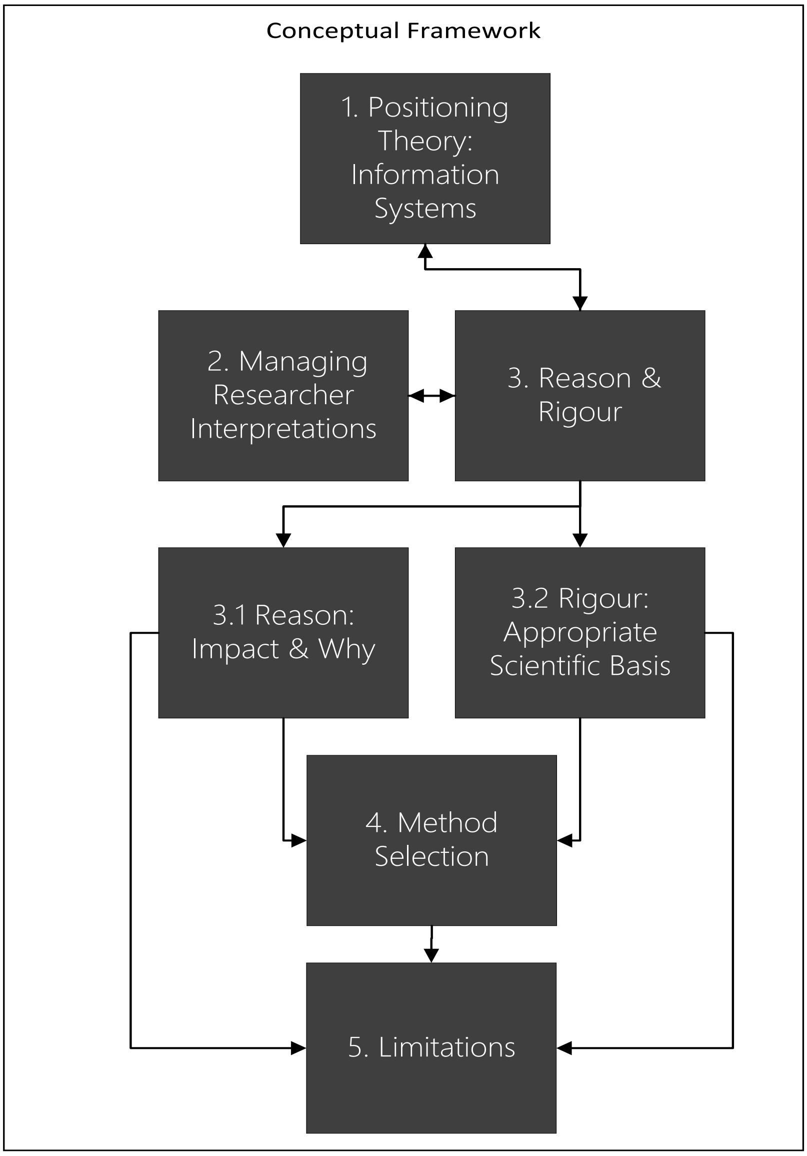

Conceptual Framework
1. Positioning Theory: Information Systems
2. Managing Researcher Interpretations
3. Reason & Rigour
3.1 Reason: Impact & Why
3.2 Rigour: Appropriate Scientific Basis
4. Method Selection
5. Limitations

Figure 6: Construction of a Conceptual Framework, distilled from Creswell, 2014; Ravitch, 2017; Rogers, 2016, Shanks et al., 1993; and Yin, 1994

These two aspects lead to the final parts of a conceptual framework, method, and limitations, which are directly informed by the positioning theory, reason, rigor, and the researchers' interpretations of requirements. As such, the method selected should fulfil all these requirements, finalizing the framework as a whole – to reiterate the aspects as described by Ravitch (2017) "…a way of linking the separate aspects within the research process; an argument as to why one wants to study a given matter and why the prescribed method is appropriate and rigorous". It should be noted that research questions are not listed here – while they do spur the start of the research, they are not directly part of the framework itself. This exclusion of the research questions from a conceptual framework is deliberate; while any method must answer the research questions, the questions are not bound to a specific method, approach, or theory.

3.1.1 Positioning Theory

The theory used within a conceptual framework shapes a researchers' outlook when interpreting the different systems and their associated interplay. The Theory of Information Systems presented by Shanks (Shanks et al., 1993) prescribes a system where knowledge, research and philosophy are related and influence the information technology systems under study.

In contrast, the analysis and overall interpretation are shaped by the systems under analysis and then related back to the overall research. Given that Information Systems are large, complex systems of systems across a myriad of platforms and interactivity levels, the malleability of the theory is both a strength and weakness (Hevner & Chatterjee, 2010).

As a strength, Information Systems (IS) theory allows for the systematic analysis of each system within the system – that is, analysis can be as granular as needed for the required outcomes of the research. The on-demand granularity allowed the research to *deep dive* on a specific system or segment as required, without sacrificing the knowledge and potential impact of interactions with the system under analysis. This layered approach allows for a system to be investigated as far as it needs to be for a given aspect or context. This variability also gives rise to a point of potential failure of Information System theory - when all aspects are interrelated and variable, the onus is on the researcher to denote the limits of the research.

Figure 7 shows the linkages between Information Technology (IT) and the different areas of research, with Information Technology at the core of the theory. As IT systems are as varied as the devices that constitute them, the outcomes and findings of a research project will vary dependent on the IT system under study – noting that an IT system is nearly always a system of systems. The theory mirrors a system of systems, as each part of practice, scholarship, reference disciplines and research must interact, compliment, and adapt to changes in other areas. Given the complicated nature of the theory of information systems, further explanation is required.

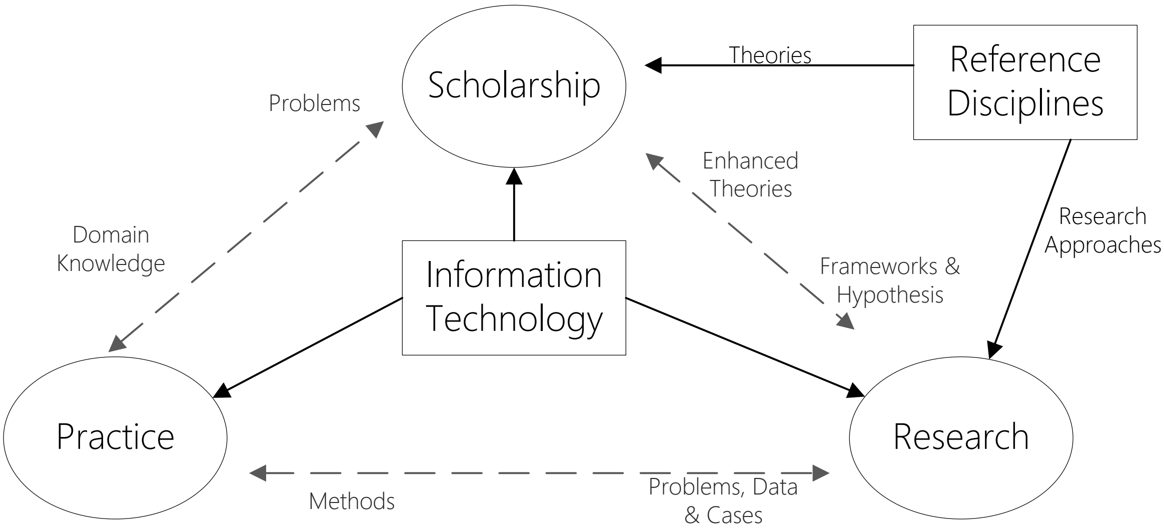


Figure 7: A Model of the Discipline of Information Systems, Adapted from (Shanks et al, 1993).

3.1.2 Managing Research Interpretation

The interpretations of the researcher touch all aspects of the research. This includes minor aspects, like language and word choices, or a documents' layout to more ephemeral aspects, such as the selection of resources and the researcher's viewpoints on knowledge generation. This expansive influence must be qualified in some fashion, lest decisions made during the process be opaque, to the detriment of the rigour of the research. As the research progresses, these interpretations evolve in a feedback loop of knowledge generation and discovery, feeding into the contextual analysis. It is impossible to separate a researcher's own views from the interpretation of research.

In following the Shanks' Theory of Information Systems, a researcher forms a part of the system when addressing scholarship (Shanks et al., 1993). This aspect of interpretation from a researcher also comes into play when making method choices – some methods (e.g., Case Studies) are more prone to criticism and flaws based on their interpretive and perceived free-form nature. To control for this issue of free-form research, there are established procedures that can inform the overall research and method.

While more detail is presented in later sections, this can be summarised in a single word – transparency. One cannot separate the interpretation from the researcher. However, the researcher can explain their logical thought process at each stage of the research, thus allowing others to see the logical flow (even if they do not necessarily agree). This transparency presents an opportunity to limit bias and subjectivity of a researcher and maintain objectivity (Dube & Pare, 2003).

3.1.3 Reason

The reason of a theoretical framework can be noted as motivation. This reason is often multivariate - a combination of a researcher's personal ambition, the influence of the research outcomes and the relevance to the wider world. Alternatively, this can be more precisely stated as 'why does the research need to be done?'. As the researcher drives the reason, it includes the researcher's own perceived impact of the research and importance to the area under study. As with all research, these pieces can be difficult to articulate at the beginning of the journey, as if we already knew the answers, there would be no research to find them – truthful, if a little hyperbolic.

The articulation of impact comes down to a researcher's best, educated guess. This estimation gives rise to some manner of uncertainty, as a researcher's hypothesis could be anywhere between accurate; to so far left of field that the original premise of the research is rendered moot. This uncertainty could lead to a conservative estimation of impact or downplaying of importance (and just as easily, overplaying) (Ravitch, 2017).

3.1.4 Rigour

The rigour of research is directly translatable to scientific rigour. As such, this is a well-understood process and section of any research project – the creation of a clear, reproducible process that; limits bias, increases the accuracy of results and allows for the independent verification of the results. This goal is supported by many institutes that have formal policies. The study of rigour has seen the classification of levels of rigour – from 'Insidious Rigour', a deliberate falsifying of data, to 'Enduring Rigour', the gold standard of independently reproducible research (Hofseth, 2018). A lack of rigour can be construed as misconduct, leading to misinformation or retraction of publication(s) (Hofseth, 2018).

3.2 METHODS

This section is prefaced by the research questions, with the discussion and selection of research methods that could answer these research questions and the justification for selecting multiple case studies as a primary method. Subsequently, the specific research design and its limitations are described.

3.2.1 Research Questions

This research aimed to answer the following questions.

3.2.1.1 *Primary*

- How do we create a framework of cybersecurity guidelines to improve the application and effectiveness of cybersecurity for the 'Internet of Things'?

3.2.1.2 *Secondary*

- How do we define the term 'Internet of Things' (IoT)?
    - Given that we have no clear system boundaries for IoT, how do we apply cybersecurity to these systems?
- Is it possible to create a categorisation schema for IoT?
    - How do we define the "Healthcare Internet of Things" (HIoT)?
- Given the unique challenges faced by the HIoT, how do we apply cybersecurity to these systems?

Like methods, not all methodologies are relevant to all research designs. Before selecting a method, the underlying methodology that a researcher subscribes to must be identified. A brief overview of the methodologies considered for this research are listed in Table 3.

Table 3: Research Methodology Overview, Adapted From (Anderson & Williams, 2017)

Research Methodology	Characteristics
Action Research	Concerned with performing an action, reflecting on the results, and then performing another action in an iterative, looping way
Phenomenological Studies	Designed to explain the difference and linkage between beliefs, preconceptions and thoughts
Multiple Case Studies	Concerned with creating multiple individual case studies that can both 'stand alone' and feed into one another
Design Science	Concerned with the development of a new artifact or system

Using Table 3: Research Methodology Overview, Adapted From (Anderson & Williams, 2017) as a base point, Table 4: Research Methodology Inclusion / Exclusion shows the suitability of each methodology and its subsequent usage of exclusion for this research.

Table 4: Research Methodology Inclusion / Exclusion

Research Methodology	Selected / Excluded	Reasoning
Action Research	Excluded	This research is not concerned with actions and the subsequent reaction, nor is the researcher embedded into a cycle of action and reflection
Phenomenological Studies	Excluded	This research is not studying a specific phenomenon, nor is it exploring what people have experienced
Multiple Case Studies	Selected	This research is concerned with an area that covers multiple discreet topics and multiple possible contextual viewpoints. Further discussion in Section 3.2.2
Design Science	Excluded	This research is not creating or developing a new system or artifact, nor is it concerned with validating a new system or artifact

The following table (Table 5) is adapted from (Anderson & Williams, 2017) and presents an overview of the research methods considered. Methods are not universally applicable to research, and careful consideration must be taken to ensure an appropriate method is selected.

Table 5: Research Methods Overview, Adapted From (Anderson & Williams, 2017)

Research Method	Characteristics
Lab experiments	Allows for the investigation of variables in a controlled and replicable environment; however, this is not always determinate of 'real-world' scenarios
Field Work	Examination of a society or organization but suffers from a lack of controls
Simulation	Observation of situations that allow for extrapolation of behaviour from known effects. This requires an accurate 'base' to be effective
Survey	Description of a situation at a given point that relies on interpretive questions. Sample sizes and selection of candidates are possible issues
Conceptual Studies	Critical analysis of a current knowledge base in terms of a belief system
Delphi Method	A series of "rounds" in which the participants (known as "panellists") generate ideas or identify salient issues, comment on a questionnaire (constructed based on the results from the first round) and re-evaluate their original responses
Participant and non-participant observation	Studies which involve observing people can be divided into two main categories, namely participant observation, and non-participant observation. Non-Participant Observation infers from a sample of

	population not under research controls, whereas Participant Observation embeds a researcher into a small group, similar to action research
Interviews	Either letting the interviewee speak freely about a particular issue or asking specific pre-determined questions. This will have been decided in advance and depend on the approach used by the researchers. A semi-structured approach would enable the interviewee to speak relatively freely, at the same time allowing the researcher to ensure that certain issues were covered
Questionnaires	Questionnaires typically contain multiple choice questions, attitude scales, closed questions, and open-ended questions. Low response rate and people do not always answer all the questions and/or do not answer them correctly
Case Study	The study of a specific person, event, place, group, phenomenon, organisation, or system

Using Table 5 as a base reference, the suitability of each method can be summarised, with further identification of potential suitability at later stages of the research. This is shown in Table 6: Research Method Inclusion / Exclusion.

Table 6: Research Method Inclusion / Exclusion

Research Method	Selected / Excluded / Later Stage	Reasoning
Lab Experiments	Excluded	Laboratory experiments with a defined set of controlled, dependent, and independent variables are not useful as the over-arching method. This is due to the research's highly contextual analysis and non-standard aspects. However, it is useful for some parts of the research when testing individual components of a solution may be required. As such, while it is not the sole method, it may be utilized at a later phase of the research
Field Work	Excluded	Field work, or the undertaking of analysis in a live environment with the researcher embedded within it, is not applicable to this theory-based research
Simulation	Later Stage	Simulation or the accurate representation of a matter that allows for extrapolation is similar to laboratory experiments
Survey	Later Stage	Surveying users or potential users of the research result could allow for further insights but again does not apply to the overall research method. It may be applicable in later stages of the research
Phenomenological Studies	Excluded	There are no phenomena to be studied in this research; as such, this method is not applicable

Conceptual Studies	Excluded	The research is not concerned with a belief system or other conceptual, faith-based analysis. As such, this method is not applicable
Delphi Method	Later Stage	The Delphi method, used to canvas subject matter experts in an anonymous fashion (Dalkey & Helmer, 1963), is not directly applicable to the research as the primary method. It has the potential to be utilized in a later stage of the research, to assess a prototype or results of the research, and to identify further work areas
Participant and non-participant observation	Excluded	As with observational trials, the research does not observe live subjects; thus, this method is not applicable
Interviews	Later Stage	The use of interviews within the social sciences is generally accepted as a key component of research design. This importance has also been noted by (Kvale, 1996) who points out that the effect of interviews is usually not observable in a direct manner. As interviews are interactive, the interviewer can refine clearer answers and divergent but relevant topics during the communication. Therefore, it can be stated that interviews allow for the broadening of scope and understanding of the subject matter in a more natural way (Alshenqeeti, 2014). However, one must take care that the disadvantages, namely that interviewing people depends on access to the person, ethical and anonymity considerations, inconstancies in recounting, and bias. As with Laboratory Experiments, Simulations and Surveys, this method could be used in a later stage to inform the completeness of a solution
Questionnaires	Later Stage	As the research is concerned with the study of devices and theoretical analysis of security concepts, the usage of questionnaires as the main research method is not feasible. However, it is possible that a questionnaire could be developed at a later stage to ascertain feedback and refinement of the research or areas of additional work
Case Study	Selected	Case Study is the overall selected method, due to the ability to capture context, analyse dynamic boundaries, and study a given system and its interaction with the set boundaries. Full discussion in Section 3.2.2

3.2.2 Selected Method

The following section is a theoretical interpretation of how to perform case studies, with the full research design in Section 3.3. The Case Study method has been selected as the most appropriate method to carry out the research in an effective and repeatable manner. The case study method has its roots in the contextual analysis of a phenomenon. The case study allows for examining a topic under multiple difference lenses – allowing a researcher to examine a bounded system from multiple viewpoints. This contextual shift is required for effective cybersecurity analysis, as a user, attacker and defender all utilise the system under examination.

This usage also means that interactions with a system must be accounted for. As this interaction is usually human based, the unique context of a given person will change how they interact with a system and thus change how any cybersecurity measures may or may not be effective. As the interactions of humans with systems and systems with systems for a complex, interrelated system, a case study allows for examination of both the system and the greater system of systems.

A case study also has enough 'give' to account for the fluidity and opaqueness of new IT-based fields. This fluidity is not to say the research itself is unclear but that the investigation area is still in a state of flux and development.

By coupling the ability to shift concepts with the theory of information systems, a case study allows for a dynamic level of analysis between cases, and the ability to perform segmented analysis of a given system, while still considering any shifts that may occur due to external systems and their influences.

This adaptability means that case studies are used in a multitude of research areas, although they originated in the social sciences. Case studies are usually deployed for "…a large variety of factors and relationships are included …when the factors and relationships can be directly observed." (Fidel, 1984).

Yin (1994) defines a case study method as an empirical inquiry that investigates a contemporary phenomenon within its real-life context when the boundaries between phenomenon and context are not evident, and multiple sources of evidence are used. There is an important distinction in the word phenomenon, as confusion can arise with the mention of Phenomenological Studies.

A case study may look at the same subject area as a Phenomenological Study and it may even come to some of the same conclusions. The key difference is that a case study is constrained to a specific context. Therefore, while the investigative bounds of a case study that may include behaviour, it is not the sole aspect that makes up the case.

Given these characteristics, a case study can be broken into a general overview that is presented in Figure 8 – a bounding box of context (the case) and a topic to be analysed from within the bounds of that context. This represents a case study in its most basic form – and is suitable as an atomic building block for the creation of different types of complex case studies.

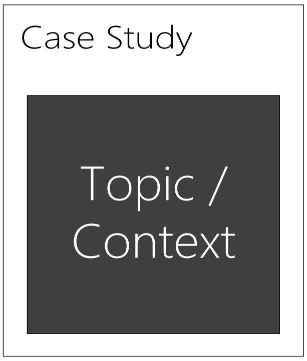


Figure 8: A Single Case Study

Instead of different types, the accurate term is tailored case studies. Each specific case study is contextually aware and is expanded to take advantage and address specific contextual requirements, although it is rare that a single Case Study can cover all aspects of a designated area. As such, the 'Embedded Case Study' was built from the need to look at multiple topics within a single contextual boundary (Scholz & Tietje, 2002; Yin, 1994). Depicted in Figure 9, this allows for multiple topics to be examined, and analysis of interrelations, between case studies within the defined area.

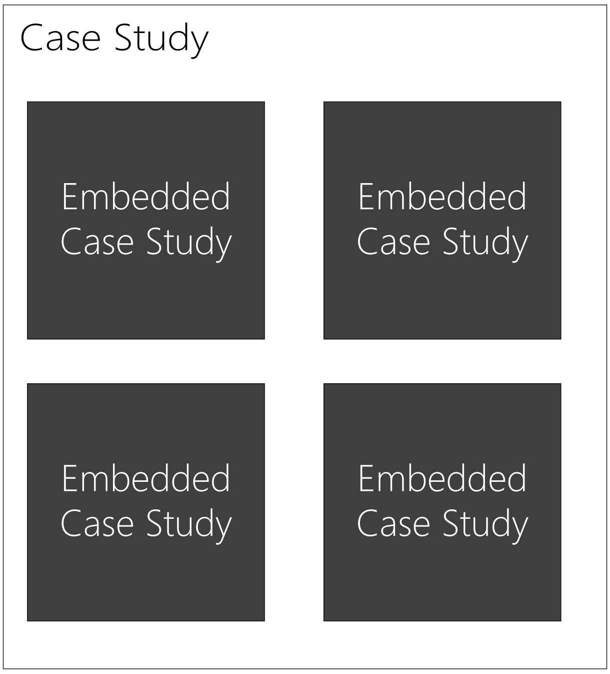


Figure 9: A Multiple Topic Case Study

This compound case study still does not adequately capture the complexity of modern-day systems of systems – or the need to examine more than one contextual outlook in an investigation. This is complexity stems from the interconnected nature of digital systems, where there are aspects of these systems that can operate in both an isolated, stand-alone manner; yet also have components that communicate and rely on other systems. Due to the ability for devices to both stand alone and be connected to a larger system, there is, at some point, human interaction – therefore, unless specially accounted for in a studies context, this interaction may be missed.

This leads us to the final and subsequently selected method. As a combination of shifting contextual analysis and multiple topic analysis, the multiple cases (sometimes called *holistic cases)* and multiple embedded topics (sometimes called *embedded cases)* allow for the capture of complicated modern digital systems (Scholz & Tietje, 2002). Depicted in Figure 10, we can see that each contextual analysis stands alone, with its defined topics – yet they are connected, as findings from one may affect the others and opening new avenues of investigation. All the case studies investigations are guided by an initial case, setting the boundaries required for the research.

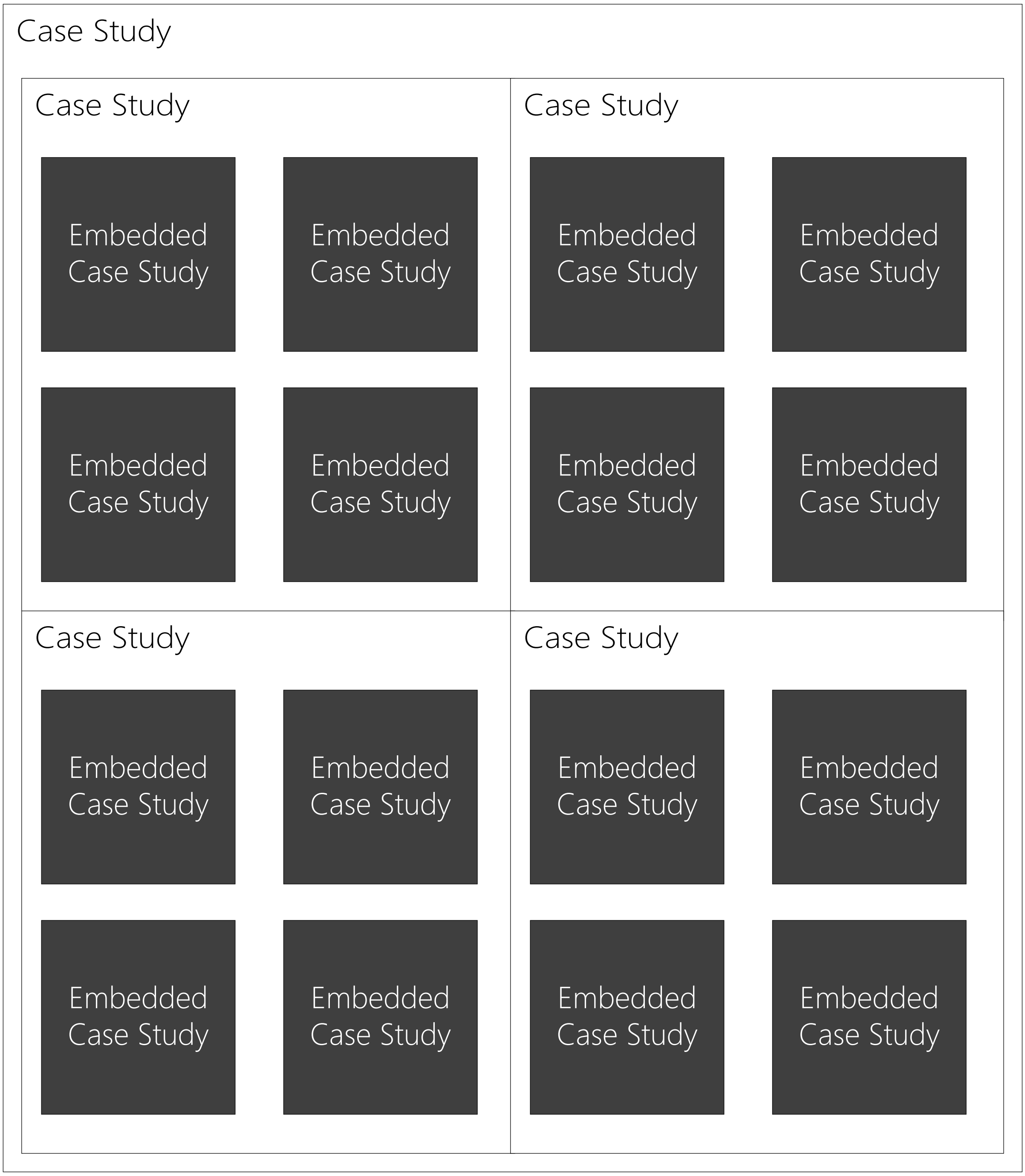


Figure 10: A Multiple Case, Multiple Topic Case Study

The selection of the methods for each approach within these multiple cases depends on their inputs and context. Each Case Study has its unique context – this context may change, as there is potential for substantial shifts between cases due to their interconnected nature. This ability to shift between cases is only possible due to the malleability of Case Studies and their ability to alter themselves to take advantage of the methods and techniques that best answer the questions without invalidating the approach to the research overall. This malleability comes at a price – the Cases must more clearly articulate their context, lest they be considered inadequate, incomplete, or lacking in rigour.

As with any research method, the case study must adhere to reproducibility and validity. Reproducibility within a case study cannot be claimed in the traditional scientific sense – the inherent nature of observation and recording events as they occur or are analysed is subjective. As such, while the analysis may be observed again – the exact thought patterns of a researcher and surrounding context will not be the same, thwarting the ability to recreate exacting circumstances for identical context. This slight difference, however, is the main point of the Case Study method - when identical events lead to similar yet slightly distinct outcomes directly due to these similarities during contextual analysis. It is this majority of agreement that defines a compelling Case Study.

The method of Case Studies follows a defined yet flexible workflow structure. It cannot be too rigid, lest the contextual analysis needs are stifled – nor can it be too loose, lest reproducibility suffer (Flyvbjerg, 2006; Thomas & Myers, 2015). There are four defined steps for a Case Study to be performed, and it is not dissimilar to any investigative analysis. These steps are:

1. Gather information
2. Apply Context
3. Analyse the findings
4. Draw conclusions

3.2.2.1 *Gather Information*

The information gathering stage is investigative and relies on the defined areas of the case. This step aims to discover all possible data about what resides within the case presented, relying on the boundaries set to prevent spending an inordinate amount of time at this stage. It must be noted that the flexibility of Case Studies allows for the return to the informational gathering processes if required at a later stage.

3.2.2.2 *Apply Context*

The application of context (also called *contextual learnings*) is where the data is applied to context to create information about the case. The application of context is where the nuances of interaction and perspective collide – generating new data, context, and information. This combination of complicated factors also creates an increase in complexity as each characteristic feeds into the others.

3.2.2.3 *Analyse Findings*

The analysis phase is not dissimilar to other methodical approaches to analysis. By taking the findings, applying the context and researchers' knowledge, analysis gathers the data, information and observations generated to create observations of what the case study has observed.

3.2.2.4 *Draw Conclusions*

As with the analysis of findings, the drawing of conclusions does not differ from other approaches. It is here the researcher draws together the analysis to answer questions and postulate the overall findings of the research.

3.2.2.5 *Limitations*

The limitations of a case study approach cover both general and specific issues. In general terms, the qualitative nature of case studies raises concerns of objectivity, as any conclusions are based on interpretation of a prescribed setting. This concern can be summarised as follows:

> "…quantitative measures *appear* objective, but only so long as we don't ask questions about where and how the data were produced… pure objectivity is not a meaningful concept if the goal is to measure intangibles [as] these concepts only exist because we can interpret them" (Berg & Lune, 2012).

As this research is concerned with creating and interpreting two distinct ecosystems (usage and security) and effectiveness in the creation of a framework, the methodology inherits the limitations of qualitative research.

This interpretation and measurement may be influenced by researcher bias. Further, as a case study looks at a single contextual instance, applying generalizations made from a single study to a broader area is a limitation to be aware of.

In addition, the method of Case Studies allows for rather free-form research. As such, this can lead to differing or conflicting methods in achieving identical outcomes. This fluidity can cause critique against the research in general, as suggested by Maoz that "the use of the case study absolves the author from any kind of methodological considerations. Case studies have become in many cases a synonym for freeform research where anything goes" (Maoz, 2002). This is an accepted issue with the case study method and must be addressed by the specific design of the case study – as such, the answer to this criticism is addressed in Sections 3.3.2-3.3.7.

3.3 RESEARCH DESIGN

The overall research design shown in Figure 11: Proposed Multi-Embedded Case Study Research Design follows the Case Study method, with a specific case layout (and therefore, workflow) described in Section 3.3.4. All cases are presented in a context agnostic manner – context will be captured and detailed by the case when undertaken, as mandated by workflow prescribed in Section 3.3.4. There are two phases of the research - the first phase is the completion of each of

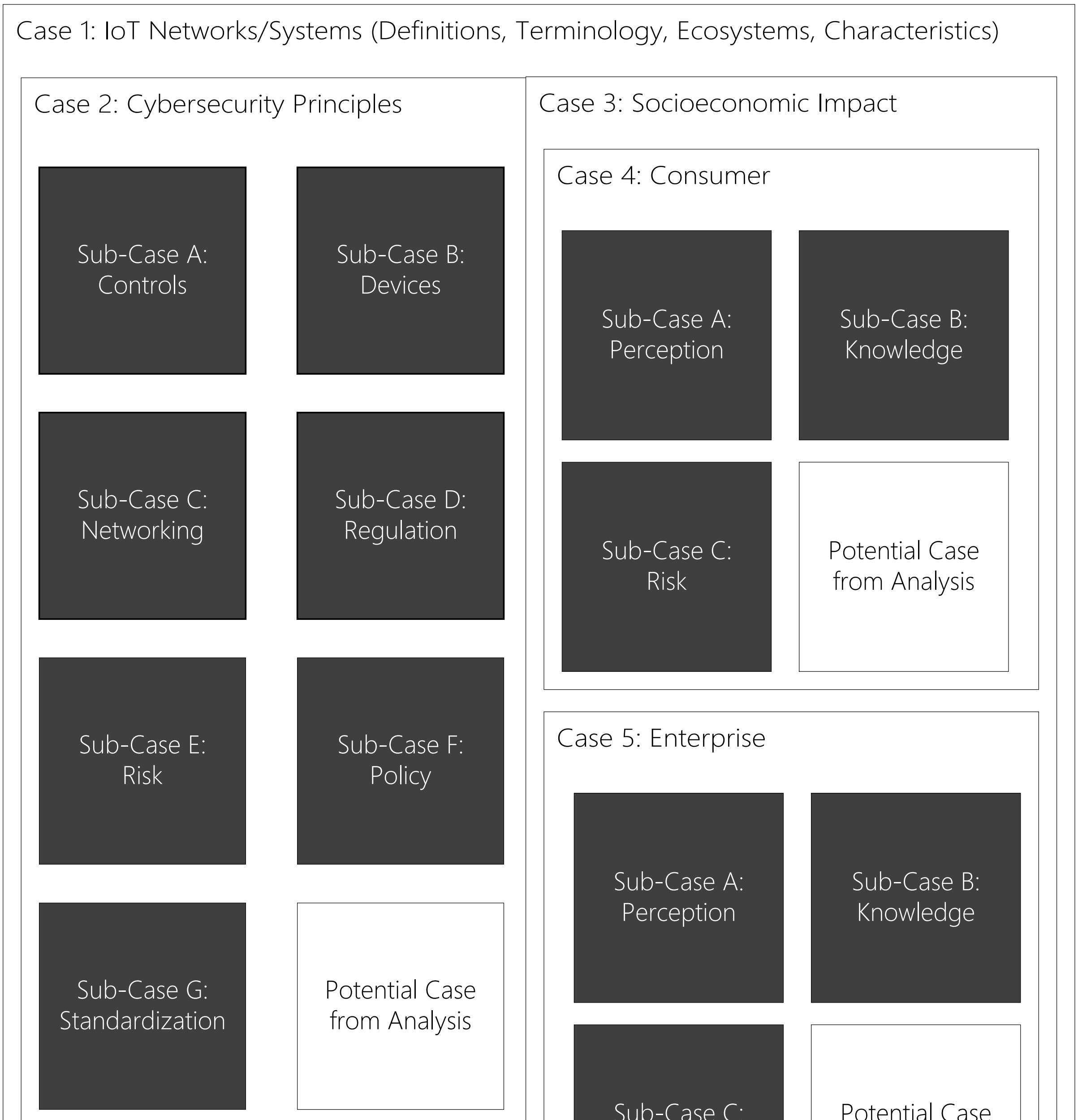


Figure 11: Proposed Multi-Embedded Case Study Research Design

the prescribed cases; the second is the cross analysis of these cases to draw additional conclusions. This two-phase approach is partly due to the research's complex and shifting nature. Therefore, the method is presented in multiple sections. The first will detail what information will be gathered in each case; secondly, the planned cross analysis of the main cases (2, 4, & 5) will be detailed. As cybersecurity is an interconnected web, each individual case builds and then layers the information to allow for examination between each case – no single case will answer a single research question due to the interconnected nature of cybersecurity – all cases contribute to answering all research questions.

3.3.1 Selection of Cases

The cases were selected to address issues identified during the literature review and to answer the research questions. Case 1 was designed to create a boundary of the overall investigative area and shape the contextual viewpoint for all subsequent investigations. This case stemmed from the literature review, as language and boundaries were identified as requiring additional clarity.

Case 2 was designed to provide clarity on the complex and multifaced problem of cybersecurity, with each sub case addressing component of the applying cybersecurity. Case 3 was designed similar to Case 1 – the need to rescope and re contextualise the investigation to look at the social and economic impact factors, not just technical factors. Finally, Case 4 and Case 5 split deliberately to investigate how the different technical requirements between consumers and enterprise impact the knowledge and interaction with cybersecurity.

3.3.2 Reason in Case Studies

Taking the uncertainty of case studies into account, the expected outcomes and impacts of this research are:

- Greater coherency of the IoT Ecosystem
- Clarity of cybersecurity measures and effectiveness within the IoT Ecosystem
- A new approach to Cybersecurity with respect to IoT devices

Greater coherency of the IoT Ecosystem will allow for identifying and categorising existing and emergent technologies. The current lack of coherency of the ecosystem is detrimental to cybersecurity, as the application of precise and effective security controls requires clear and identifiable boundaries, which is noticeably missing in IoT deployments.

While this lack of clarity in architectural layout is an understood issue in other areas of computing (e.g., Cloud Computing) the intersection between the characteristics of IoT devices and the subsequent change in cybersecurity measures is an unknown and potentially detrimental to cybersecurity efforts.

The current cybersecurity measures that can be applied in IoT are relatively new, less than five years old for most of the major frameworks, leaving traditional cybersecurity techniques (Section 1.1) applied outside of IoT languishing. As technology is evolving at a rapid pace, cybersecurity protections are in a perpetual state of 'catch up' as the devices developed and implemented are outstripping the cybersecurity protection methods available.

These issues require a new approach to cybersecurity in IoT to alleviate the rapidity of development without losing the effectiveness of protective measures. This necessitates not 're-inventing the wheel', where known and understood cybersecurity techniques are still effective in their application and instead focussing on the areas of cybersecurity that require modification to account for the unique aspects of IoT.

3.3.3 Rigour in Case Studies

The application of rigour to the Case Study method is multifaceted, and any argument made for rigour must address multiple areas.

The Case Study method has been utilized within multiple disparate and overlapping fields of research and has been well tested and understood since the 1970's (Savolainen, 1996). This extensive use alone does not provide or prove rigour. However, it allows for showcasing the greatest strengths of Case Studies – they are highly malleable and can be tailored to fit a wide range of research approaches, theories, and methods (Creswell, 2014; Ravitch, 2017). This malleability means that the Case Study can, when designed with rigour, lean on the established methods that have been proven to adhere to the level of rigour required by each Case Study, with the onus on the researcher to argue the point of 'rigorous enough' (Ravitch, 2017). This malleability is also the Achilles' heel of Case Studies. When too flexible, it can lead to free-form research that does not present a level of rigour that allows for third-party reproduction (Anderson & Williams, 2017).

There has been some argument over what exact scientific model to utilize and what constitutes the fundamental criteria for assessment of rigour when utilizing the Case Study method. In this research, the concrete research actions adapted for Case Studies from Yin (Yin, 1994) are used and further discussed and expanded by both interpretivist and positivist publications. By grouping the derived traits into four distinct categories, a definitive set of actions to be taken that provide rigour to a case study are defined (Borman et al., 1976; D. T. Campbell & Stanley, 2015; Cook & Campbell, 1976; Eisenhardt, 1989; Guba et al., 1994; Kidder, 1986; Kirk & MIller, 1986; Savolainen, 1996; Silverman, 2005, 2006). These categories, discussed below, are *construct validity*, *internal validity*, *external validity*, *and reliability*.

3.3.3.1 *Construct Validity*

The construct validity of a procedure refers to the extent to which a study investigates what it claims to investigate, that is, to the extent to which a procedure leads to the accurate observation of reality (Guba et al., 1994). Given the malleability of Case Studies already discussed, one of the critical issues in creating construct validity is creating a defined set of actions to perform instead of a set of subjective judgments (Yin, 1994). This construction of predefined characteristics disagrees with some qualitative measures, as they do not always fit neatly into a defined set of characteristics. This lack of definable and repeatable characteristics creates difficulty in obtaining common ground with quantitative research perspectives regarding the objectiveness of knowledge (Silverman, 2005, 2006).

The positivist literature suggests that existing data collection and analysis theories can be applied to Case Studies. A key aspect of construct validity is triangulation, using multiple data points and data sources to allow corroboration across investigation points (Guba et al., 1994; Jick, 1979; Pettigrew, 1990; Savolainen, 1996; Yin, 1994). In conjunction, a clear chain of evidence to articulate the limitations, timeframes, difficulties, and impacts of data collection on the research prevents hidden decisions.

This research performs the above by reporting data collection circumstances, such as organisational access and time frame. As authors are encouraged to be explicit about how the planned data collection differed from the actual process, explanations of difficulties, how this impacted results, and how such difficulties were contained or accounted for, this information is also presented where possible (Geertz, 1973).

3.3.3.2 *Internal Validity*

Internal validity is synonymous with logical validity and refers to the causal relationships occurring betwixt variables and results (Cook & Campbell, 1979; Yin, 1994). Whilst the previously stated construct validity is concerned with collecting data, internal validity is concentrated around the data analysis phase – although many decisions shaping the internal validity are made during the research design (Yin, 1994). The two main philosophical approaches of positivism and interpretivism to research share some common ground in this case. Both can be ascribed to critical realism described by Popper (2005); a researcher must continually attempt to refute beginning assumptions. Only if these assumptions cannot be refuted is the research valid (Popper, 2005).

Silverman suggests that two core concepts must be kept in mind – validity and reliability (Silverman, 2006). Whilst not mentioning internal validity directly, it is ascribed that the main contention point is to avoid cherry-picking data – anecdotalism as described by Silverman (2006). To prevent this, methods such as the constant comparative method (Glaser & Strauss, 2017) or the usage of multivariate analysis to avoid spurious correlation should be used. In contrast, the quantitative methods focus more on how the method was constructed and how the analysis is performed in a statistically sound manner (Yin, 1994).

This research maintains internal validity by discussing relationships between new data and previous research. Additionally, theory triangulation enables a researcher to verify findings by adopting multiple perspectives (Yin, 1994). In this case, authors are encouraged to report different theoretical lenses and bodies of literature used as research frameworks to guide data gathering and analysis or as means to interpret findings.

3.3.3.3 *External Validity*

External validity, or generalization, is prescribed as the requirement that any theory must be able to account for the object of study outside of its prescribed contextual setting. This applicability outside the prescribed area is hampered when any statistical analysis is required, as both single and multiple Case Studies are insufficient for first-order statistically provable generalization (e.g. population forecasts) (A. S. Lee & Baskerville, 2003; Numagami, 1998; Yin, 1994). However, this unsuitability for statistics generation does not absolve Case Studies from the need for external validity. The key is to focus instead on analytical generalization instead of statistical generalisation. This research is not performing statistical generation; instead, the analytical generalisation may take the approach of cross-referencing multiple case studies from varied sources to construct a theory (Eisenhardt, 1989) or a nested approach of multiple Case Studies within a single area (Yin, 1994).

This research creates external validity by articulating the requirements and reasoning behind the selection of each case study, including its potential industry areas. This exposition of reasoning and an explanation of any specific contextual nuances will allow readers to follow the choices made in selecting cases and investigative areas, even if the reader does not agree (Cook & Campbell, 1979).

3.3.3.4 *Reliability*

Reliability refers to removing random errata, enabling other researchers to faithfully reproduce the research (Guba et al., 1994). The removal of errata causes some contention in qualitative studies, as Silverman points out that the reader must "depend on the researcher's depiction of that was going on" (Silverman, 2005). The need for explicit descriptions creates an area where a researcher's underlying assumptions may not be articulated, decreasing the reliability of the research. While no research can be free from these underlying assumptions, some approaches can decrease the impact of not articulating these assumptions. As case studies are interpretive in nature, demonstrating the reliability of a case study can be stated as transparency. Explicit statements of data sources, analysis techniques, contextual outlooks and expected outcomes at each stage of the research allow for the data and analysis to be undertaken by others, even if their overall interpretation is different.

This research ensure transparency by exposing the listed points – the sources of data, the comparisons, expected outcomes and contextual outlooks during each case. This is done via precise case construction, requiring the exposure of this information before commencing the case content.

3.3.3.5 *Conclusion to Rigour in Case Studies*

In conclusion, it can be stated that a rigorous Case Study is somewhat more conversational, exposing the thought process of the researcher including the clearly written exposition of

> *…setbacks and serendipities that necessitated changes to the originally planned research procedures are problematized, focusing squarely on the concrete research actions taken, carefully relaying them to the reader so that he or she may appreciate the logic and purpose of trade-off decisions in the context of the specific case study* (Gibbert & Ruigrok, 2010).

This correlates to a potentially less cohesive research design and flow. Each step taken, the decision, factors and inputs are articulated so that while another researcher may interpret the same context differently, the logic behind the decision is exposed. This exposition of internal processes creates the rigour that Case Studies depend on.

3.3.3.6 *Case Study Workflow*

A good case study is like a narrative, where the researcher articulates the story of discovery and explains the decisions made along the way. This narrative approach leads to a case study that spends time performing what can be amounted to exposition as part of its workflow. At each stage of the case study, there are a multitude of factors in play – stemming from the specific subject of the case; these factors include everything from the researcher to a device under study. Case studies are geared toward studying real-world phenomena, but these factors are rarely clear to place on paper, given their ephemeral nature. This capturing of the ephemeral is a challenge, as the decisions made at a certain point could be challenged if the surrounding context and knowledge were not exposed to the reader. Given this, the workflow for the proposed Case Studies is modified to explicitly expose the internal voice and surface the decision-making process and reasonings to the reader. This newly expanded workflow is:

1.) Gather information
    a. List locations, reasoning & context of each location of data
2.) Apply Context
    a. Describe contextual restrictions, links, and inputs from other parts of the research.
3.) Analyse Findings
    a. Articulate analysis with reference to context and perspective
4.) Draw Conclusions
    a. Describe restrictions, issues, new directions, any invalidated research views and clarify the next contextual aspect to be investigated

The final stage of the research using multiple cases studies is to take the individual aspects that have been investigated and link all of them together – to create an overall picture that combines the smaller contextual areas into an overarching view that creates a broader generalization and helps to avoid the overspecialization of solutions.

3.3.4 Case Study Layout

The case study layout (Table 7) was devised to minimize the ability to omit a step and ensures each case's clarity by addressing the reason, rigour, and workflow.

Table 7: Case Study Layout

Heading	Step Number	Reasoning
Rationale and Background / Introduction	1	Why this case exists, including additional background information pertinent to the case
Contextual Notes	2	The contextual notes describe the context around the case, including differences between any previous contextual outlook of cases
Case-Specific Inputs	3	From other cases, are there any inputs required for this case
Expected Case Outputs	4	What artifact, knowledge or information is envisioned as the output from the case
Case Content & Analysis	5	The content of the case, adhering to the prescribed methodological constraints
Conclusion	6	The conclusions that can be drawn from the case
Issues Encountered During Case	7	What issues (if any) were encountered when performing the case
Invalidated Research Views	8	Were any assumptions or research views disproved during the case
Learnings from Case	9	What was learnt during this case and any potential points that feed into any subsequent cases

3.3.5 Design of Cross Analysis of Cases

Taking the compiled data from all previous cases (2, 3 & 5), a cross-analysis and comparison can now be performed. By contrasting sub-cases cases (e.g., Controls to Devices) and comparing between cases (Cyber Principles to Consumer Impact), the research will highlight the issue present due to this native crossing of contextual understandings. At the end of the analysis, this will become a list of the key issues. This will allow for a more targeted solution to address only the apparent issues and allow for the deeper analysis of only the needed areas – avoiding those already covered or sufficiently understood.

3.3.6 Multiple Case Study Design

Due to the interpretative nature of Case Studies, without adherence to strict, explicitly stated justifications of reason and rigour, the research may not be reproducible. The methodology of multiple cases studies is also the process of conducting multiple case studies. By constructing a series of cases that adhere to the requirements of a sound case study (reason, rigour, and validity), research following this process can segment a large topic area into smaller, more focused topics. This segmentation is arbitrary, in line with the nature of case studies, and reflects how the researcher believes that the topic should be investigated. This seemingly arbitrary segmentation is the expected outcome of utilising the multiple case study process, as case boundaries will be defined by the researcher. However, this definition of boundaries does not absolve the researcher of designing cases that adhere to the methodological requirements.

The strengths of the multiple case study process, the ability to use multiple contextual views, also comes with a potential pitfall. A case layout should specifically state the contextual view of each case and sub-case. The risk is, that if each specific contextual view is not stated, there is a risk of losing the nuance that defines the case or sub-cases. This is especially true when subdividing an existing case to look at the same question from a different angle, where the difference may only be slight.

In this research, each case addresses specific aspects of the IoT ecosystem and allows for cross-analysis between cases. The following case descriptions are a general overview of what each case aims to capture, with detailed case design for each case contained in Section 3.3.7. Case 1, IoT Networks / Systems, the overarching ‘umbrella’ case, addresses the need for research bounds by identifying the definitions, terminology, ecosystem, and characteristics for and within the IoT

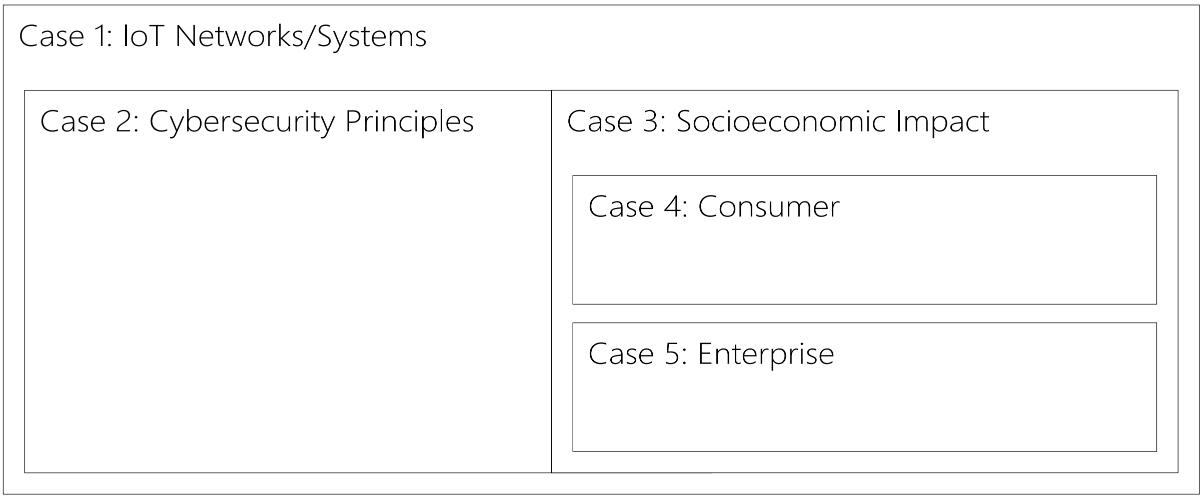

Case 1: IoT Networks/Systems
Case 2: Cybersecurity Principles
Case 3: Socioeconomic Impact
Case 4: Consumer
Case 5: Enterprise

Figure 12: Overall Research Design of Cases

ecosystem. Case 2, Cybersecurity Principles, aims to identify the technical controls, guidance, and knowledge for the application of cybersecurity within the IoT ecosystem as defined by Case 1. Case 3, Socioeconomic Impact, is similar to Case 1 in that it serves to define an investigative area for subsequent cases. Case 3 aims to identify the broad social and economic factors influencing the IoT ecosystem. Case 4 aims to narrow the focus of Case 3 by focusing on consumers. Case 5 follows the same focus narrowing but instead targets larger enterprises. These successive contextual shifts and distinct topics are visualised in Figure 12: Overall Research Design of Cases.

3.3.6.1 *Case 1: IoT Networks/Systems*

IoT and networks are the boundaries for all subsequent investigations. As such, it has the broadest scope. As Case 1 'sets the stage', it focuses on identifying what to investigate and, just as importantly, what not to investigate. Case 1 identifies the language and boundaries of what is considered IoT and begins the categorization of devices into logical groups, where possible, to aid in splitting the analysis into smaller logical chunks during the sub-cases. It is also concerned with the technologies and broad implementation differences within IoT, effectively capturing a snapshot of the ecosystem in its current state, including common characteristics.

3.3.6.2 *Case 2: Cybersecurity Principles*

Case 2 aims to look at the technical aspects of cybersecurity and compare it against known international standards and contemporary best practice, guided by Case 1. Case 2 aims to discover how IoT is protected compared to more traditional systems. It is expected that the existing body of knowledge (EBoK) will extrapolate to IoT with minor adaptation, allowing this case to identify the cybersecurity areas that warrant further investigation for issues specific to IoT. This comparison process will also identify the areas where the EBoK works well and does not need modification for IoT networks and systems.

3.3.6.3 *Case 3: Socioeconomic Impact*

Case 3 is concerned with setting the stage for further social impact drivers, similar to Case 1. Case 3 aims to identify the drivers and factors that influence the adoption, usage, and development of IoT technologies and devices from a social viewpoint instead of a technical one.

3.3.6.4 *Case 4: Consumer Socioeconomic Impact*

Consumers have, and expect, different functionality of IoT devices and their associated systems than enterprises. Case 4 specifically targets consumer-grade hardware that is deployed by general, non-professional users. By examining a consumer’s requirements and expectations of an IoT device, an analysis of the differences between IoT devices and their subsequent cybersecurity protections can be performed.

3.3.6.5 *Case 5: Enterprise Socioeconomic Impact*

Enterprise-grade hardware comes with a different outlook and technological landscape to consumer devices. As such, case 5 investigates the precise needs of enterprise applications and the viewpoint enterprises take on IoT deployment to complete the picture of IoT across the ecosystem.

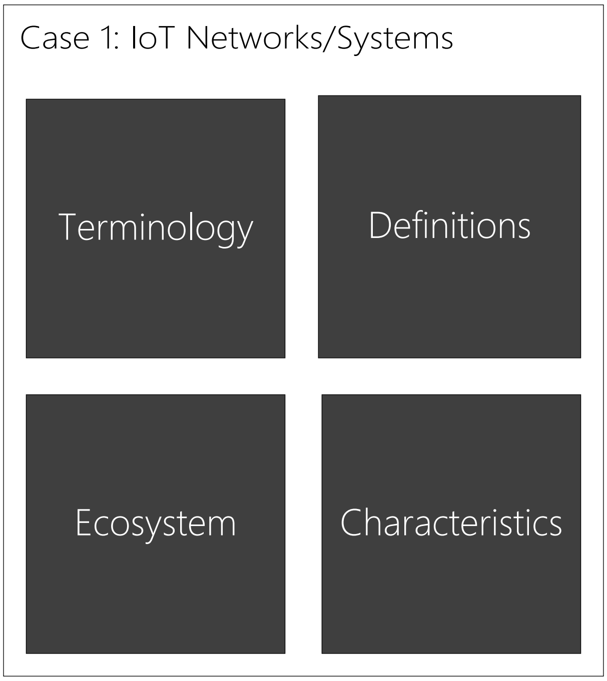


Figure 13: Case 1, IoT Networks/Systems Overview

3.3.7 Detailed Case Design

Given the complicated and expansive research design, the following sections detail each case's additional context and guiding questions. This additional information on the exact goals of each case is required to adhere to the previously stated rigour in case studies by exposing each cases’ expected goals and expected outcomes transparently. The detailed design for “Case Content” from Table 7, Step 5.

3.3.7.1 *Case 1: IoT Networks / Systems*

The ecology of the Internet of Things is mired by imprecise language and disparate ideas of what IoT is. As such, before commencing analysis identifying just what the IoT is, what words are used to describe it, and the differing characteristics of any similar deployment types must be identified. The contextual outlook for this case is the ecosystem of IoT as a whole – from the firmware on the device to platforms facilitating IoT based applications. This case forms the foundation for all cases to follow, along with the foundation to answer the research questions posed in Section 3.2.1, directly addressing the research question of “Given that we have no clear system boundaries for IoT, how do we apply cybersecurity to these systems?”. The overview of this case’s topics is shown in Figure 13.

- What is IoT?

The IoT, as a concept, is analogous to: "A small device that communicates over the internet". For a conceptual understanding of the subject area, this is sufficient. However, this shallow understanding precludes specific analysis as the language used to describe it is fractured, with multiple terms used to refer to similar concepts within the ecosystem. This case aims to apply the findings and draw definitive boundaries around IoT and any present sub-categories.

- How do we define IoT?

By drawing on the literature and the specific analysis from the terminology sub-case, this case aims to ascertain if current definitions of IoT are adequate to capture the realities of a highly diverse and fluctuating ecosystem. The resulting definition will serve as a decisively indicative test of whether a specific device or program of other usage lies within IoT.

- Is there agreement on the terms used to describe IoT?

While the point of disparate terms in IoT has been identified as an issue, not all the terms may disagree. As such, identification of the common terms will also allow the identification of common aspects between the terms. This identification of terms and their commonality will allow a matrix of 'term to aspect' to be created.

- What are the characteristics of IoT?

In conjunction with a definition, the creation of a list of characteristics and their interrelations will create a clearer view of limitations, as a definition alone fails to capture the nuances of a complicated ecosystem. This clarity of IoT characteristics allows for testing any aspect of IoT against the created definition, as a characteristic may include a given device whilst the definition precludes it.

- Can we identify distinct approaches to IoT?

As with traditional computing, distinct computing areas have emerged - for example, Cloud Computing. Each of these areas has its own well-understood characteristics, terminology, and interrelations with other distinct areas of computing – using Cloud Computing as an example, these distinct areas are PaaS, IaaS, SaaS and XaaS. IoT is almost assured of having the same strata of differing aspects; identifying these is required to address cybersecurity adequately.

3.3.7.2 *Case 2: Cybersecurity Principles*

The next largest contextual area, the identification of cybersecurity principles, requires the conjoined analysis of dynamic 'best practice' and the specific contextual guidance that comes with cybersecurity. This section will create and compile a global list of principles that are applied and well understood within cybersecurity. The sub-cases that comprise this investigative area are shown in Figure 14: Case 2: Cybersecurity Principles Overview. A set of questions will drive the investigation of each sub-case, and due to the interconnected nature of cybersecurity, there will be some crossover between the sub-cases. It is important to note that this crossover means that elements from other sub-cases may appear in a given case, even though they are not the focus.

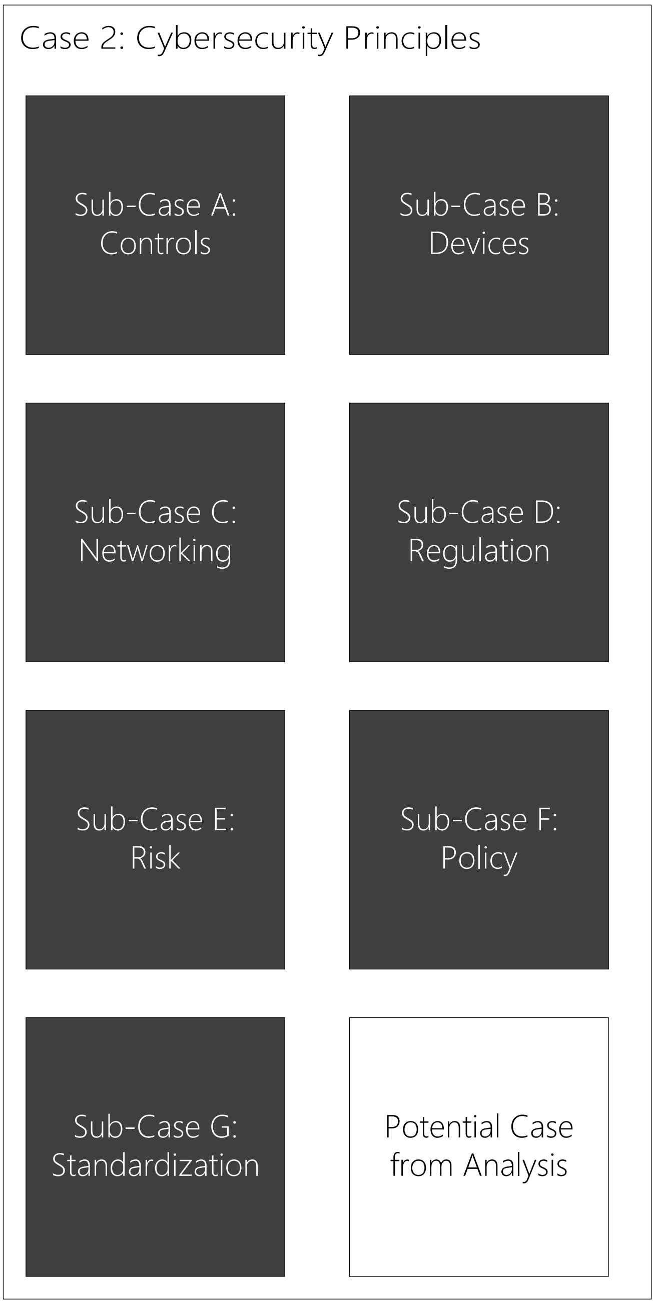


Figure 14: Case 2: Cybersecurity Principles Overview

3.3.7.2.1 Case 2, Sub-Case A: Controls

Case 2, Sub-Case A, is concerned with the technical controls that could be implemented on IoT devices. These controls will map to one or more of the cybersecurity principles. The questions that drive this sub-case are as follows:

- What Technical Controls for IoT exist?

A comprehensive list of potential technical cybersecurity controls can be created by canvassing prescribed frameworks and existing cybersecurity standards, both those specific to IoT and not. This list can be further analysed with respect to the individual aspects below.

- What is best practice?

Best practice for cybersecurity is well defined for traditional computing areas. However, the devices and relative infancy of IoT means that best practice is not well defined. As such, creating, adapting, or editing best practice guidelines will allow for the identification of current IoT best practice.

- What is the ideal best practice in IoT?

Using the best practice guidelines developed in the research, the notion of an ideal level of security can be explored. Whilst it may not be perfect, the theoretical level of ideal protection can be articulated.

- What gets implemented?

It is expected that not all controls are implemented within a given deployment of IoT for multiple reasons, ranging from time and money to technical know-how. To analyse the gaps between what is considered ideal and what is implemented, the controls implemented in production systems must be ascertained.

- What technologies are used?

The IoT is made up of a multitude of hardware and software – each with its own unique strengths and weaknesses. As each piece of hardware can be specified as unique in some way, so it is unfeasible to address each part of the device individually. As such, we must identify the core technologies that underpin devices; by identifying these core technologies, they can be genericised, and a level of abstraction can be created. This abstraction makes the application, identification, and mapping of core cybersecurity principles to IoT technologies more broadly applicable.

- What technologies were created just for IoT?

As stated, IoT devices are unique – this also means that the devices contain aspects that are not standardised. Due to this lack of standardisation, these unique aspects must be captured and considered to adequately apply cybersecurity, lest the application of effective cybersecurity is left with an unknown deficiency.

- What things are impossible on IoT?

It is clear from the technical capability of IoT devices and their natures that some aspects of modern cybersecurity are impossible due to technical limitations and others are simply unfeasible. Identifying what a typical IoT device is incapable of regarding cybersecurity is required, as these must not be included in the best practice guidelines. These are, at this stage, deliberately broad and intended to be cross-examined at a later stage.

- Additional Cases found from the analysis?

Due to the study of different areas of IoT, new cases that still apply to the current contextual outlook may become apparent as the research progresses. These new investigative areas could potentially block the progression of work until they are investigated – thus, the method accounts for this to occur N-Times with the researcher responsible for ensuring that the project moves forwards overall even if it is not in the initially planned direction.

3.3.7.2.2 Case 2, Sub-Case B: Devices

As demonstrated in both the literature review, there are many IoT devices, covering a swathe of forms and functionality. Case 2, Sub-Case B, aims to reduce this diverse range of unique devices to a set of core characteristics and capabilities. This categorisation will allow for generalisation and extrapolation that is tailored to IoT, which is critical for cybersecurity and networking at scale.

- What IoT Devices Currently Exist?

What IoT devices are currently deployed - conceptually, they are anything; however, this is not a helpful level of identification. Sensors of many types, automated pumps, smart monitors, gateways, and others are currently in usage – identification and categorisation of IoT that is currently deployed and in active usage is the goal of this case.

- How do we refine or create new IoT categories?

Using the work on terminology to start with broad categories based on the linguistic analysis and the knowledge of devices will allow the refinement of the initial IoT categories. This refinement may expose subcategories based on devices or characteristics.

- What are the limitations of IoT Devices?

The devices that are identified will have a set of common computing characteristics. Identifying these will allow for devices to be grouped by function and relative performance concerning computing tasks.

- Unique devices and their characteristics

The diverse and dynamic ecosystem of IoT lends itself to unique devices. It is expected that there are unique aspects to IoT devices that will need to be quantified in some manner – the level of uniqueness may allow for some abstraction away from specific devices. This echoes the analysis of the unique aspects of cybersecurity for the IoT ecosystem but is instead focused on IoT devices.

- What Operating Systems are used in IoT?

Operating Systems is a large subject and must cover embedded firmware and traditional operating systems deployed over a network. What operating systems are on IoT devices is of great import to cybersecurity, as the Operating System forms the foundation of all later protections. Identifying these operating systems will also allow for the analysis of any additional cybersecurity concerns that may arise from the types of operating systems present in the IoT ecosystem.

3.3.7.2.3 Case 2, Sub-Case C: Networking

IoT Networking draws heavily from the well-established Cloud Computing paradigm. Case 2, Sub-Case C, aims to analyse the different protocols and methods invented to tackle the unique challenges of networking IoT devices.

- What protocols are used in IoT?

IoT's diverse nature has spurred the creation of many different protocols for different IoT deployments. Many of these protocols are proprietary and provide the same functionality in different ways. These protocols are also targeted at different aspects of IoT – some for connectivity, others for security, and others for messaging. A clear picture of the protocols' strengths, weaknesses, and features is required before cybersecurity protections can be applied. The identification of these protocols and their specific strengths and weaknesses allow cybersecurity measures to be targeted at deficient areas.

- Variation in overall layouts

The differing network layouts will be closely aligned with their selected approach (2.3.1.1); however, significant variations exist within each paradigm due to business, networking, device, and other constraints. These variations will need to be quantified to apply cybersecurity measures effectively.

- How do existing network layouts impact IoT?

As IoT is highly influenced by existing technologies and deployment types, by using the robust existing body of knowledge for cybersecurity, this investigative area aims to pinpoint the cybersecurity concerns that are already known regarding the existing deployment paradigms (used for IoT) and how they are magnified, mitigated or otherwise when IoT is layered on these existing networks.

3.3.7.2.4 Case 2 Sub-Case D: Regulation

Regulatory bodies are not ignorant of the risk that IoT devices present. Initial frameworks for cybersecurity of IoT devices are being published regularly (H.R.1668 - 116th Congress (2019-2020), 2020; *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Measures for a High Common Level of Cybersecurity across the Union, Repealing Directive (EU) 2016/1148*, 2020), with some prescribed as wanted or mandatory by governmental bodies, similar to existing cybersecurity standards. A practical cybersecurity framework must align to these standards if it wishes to be applied to the real world, where benefits must be tangible.

- What are the existing regulations, guidelines & industry standards?

As regulations differ in scope and focus across national and international jurisdictions, there is a need to capture the existing regulations, standards and guidelines that exist to guide IoT devices and networks. These documents demonstrate IoT's thinking and overall direction and allow any differences between industry self-regulation and governmental legislation to be highlighted.

3.3.7.2.5 Case 2 Sub-Case E: Risk

Risk is a widely understood measure in cybersecurity and a staple of all existing cybersecurity operations. Case 2, Sub-Case E, aims to build on the well-understood area of cybersecurity risk frameworks and ascertain their usefulness against IoT.

3.3.7.2.6 Case 2 Sub-Case F: Policy

Policies set by the government can have a significant impact on any given technological ecosystem. Case 2, Sub-Case F, is concerned with what federal level policies have been set by any of the Australian, European Union, or United States of Americas' governments. There are also potential proprietary policies that technology leaders have published (e.g., Apple, Microsoft) that may have seen significant adoption. This case with these policies, if they are published and how they compare to the wider standards and legislations – including how they are marketed and can be adopted by the wider technical community as de facto standards.

3.3.7.2.7 Case 2, Sub-Case G: Standardisation

International standard bodies, notably the International Organization for Standardization (ISO) and The International Electrotechnical Commission (IEC), publish widely adopted and referred to standards within the cybersecurity area. National standards are those published or adapted by a national or governmental standard body (e.g., Standards Australia). Only Australia, the European Union, and the United States of America were considered potential candidates to keep the research scope to a reasonable level.

The focus of standards can vary widely, from technical guidance to risk assessment profiles. As such, it is not sufficient to say that a standard exists; it must also be understood in what context it is applicable. The identification and categorization of National and International standards and their focus will occur in this case.

3.3.7.2.8 Design of Cross Analysis of Case 2

Case 2, Cybersecurity Principles (3.3.7.2) requires internal cross-analysis, as each sub-case intersects heavily with one or more cases. As such, internal cross-examination of the individual sub-cases is required to shed light on additional potential issues caused by these intersections. As the full titles of these cases are unwieldy to repeat ad nauseum, Table 8 shows the short codes used to refer to the individual sub cases, their full title and overall topic of study. Table 9 then shows the list of comparisons between cases using these short-codes, as well as a short description and the expected outcome from the cross analysis.

Table 8: Case 2, Cybersecurity Principles Analysis Short Codes

Case Identifier	Full Case Title	Topic
2A	Case 2, Sub-Case A: Controls	Cybersecurity Principles: Controls
2B	Case 2, Sub-Case B: Devices	Cybersecurity Principles: Devices
2C	Case 2, Sub-Case C: Networking	Cybersecurity Principles: Networking
2D	Case 2, Sub-Case D: Regulation	Cybersecurity Principles: Regulation
2E	Case 2, Sub-Case E: Risk	Cybersecurity Principles: Risk
2F	Case 2, Sub-Case F: Policy	Cybersecurity Principles: Policy
2G	Case 2, Sub-Case G: Standardisation	Cybersecurity Principles: Standardisation

Table 9: Case 2, Internal Cross Analysis Overview

Comparisons	Description	Expected Outcome
2A to 2B,C,D,E,F,G	Take the cybersecurity controls of 'best practice' and ascertain how they are applied according to all other sub-cases	Conclusions as to how cybersecurity is applied across a broad range of areas – and more importantly, where it is *not* applied
2B to 2C	Take the devices, their core characteristics and networking communications, comparing to cybersecurity strength and weaknesses from the first cross-comparison	A grouping of IoT devices and their common networking protocols, capabilities, and approaches, including common areas of deficient cybersecurity predictions
2B to 2D,E,F	Take the devices and compare their characteristics to current and upcoming risk, regulations, and policy documents regarding cybersecurity	An understanding of how IoT currently conforms to known (and upcoming) risk, regulation, and policy documents
2B to 2G	Take the devices, and ascertain how devices are adhering to any standardisation efforts, and what impact that has on cybersecurity for IoT	An understanding of how IoT is being affected by standardisation efforts, and how these standardisation efforts are affecting the cybersecurity measures in the IoT ecosystem.

3.3.7.3 *Case 3: Socioeconomic Impact*

Case 3, Socioeconomic Impact, is concerned with the drivers of consumerism and the potential feedback this may have on the IoT ecosystem. Case 3 is similar to Case 1 in that it is both an investigative piece and sets additional boundaries for subsequent research. Due to this case being concerned with setting boundaries, this case is primarily concerned with the broad principles of consumerism, the possible feedback methods, and factors to IoT, and the potential avenues for investigating IoT's Socioeconomic Impact. The overall structure of this case is shown in Figure 15.

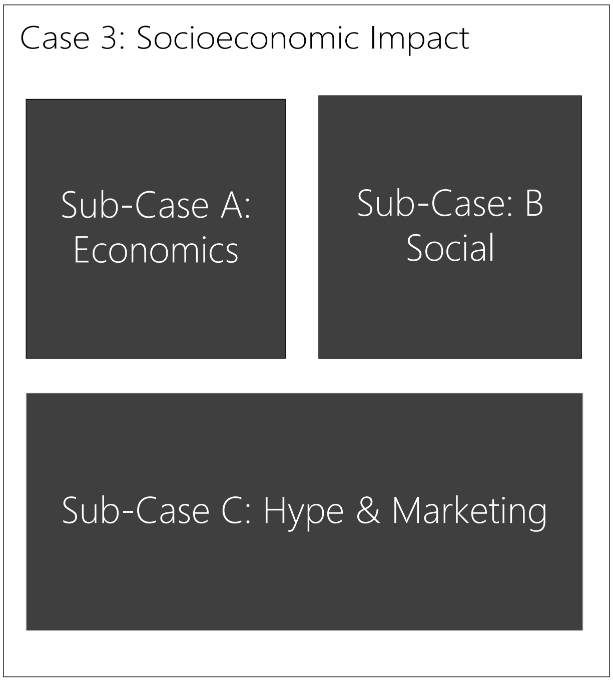


Figure 15: Case 3: Socioeconomic Impact Overview

3.3.7.3.1 Case 3 Sub-Case A: Economics

Case 3, Sub-Case A: Economics is concerned with the economics factors that influence the adoption, usage, deployment, and protections of IoT devices and their associated networks.

3.3.7.3.2 Case 3 Sub-Case B: Social

Case 3, Sub-Case B: Social is concerned with the social factors that influence the adoption, usage, deployment, and protections of IoT devices and their associated networks.

3.3.7.3.3 Case 3 Sub-Case C: Hype and Marketing

Case 3 Sub-Case C: Hype and Marketing is concerned with how expectations and social pressures, expectations and the 'hype' factor can influence the adoption, usage, deployment, and protections of IoT devices and their associated networks.

3.3.7.4 *Case 4: Consumer*

Consumers are rapidly adopting IoT, and smart devices are now commonplace, if not ubiquitous. Consumers' adoption of these IoT devices means that they must 'just work'. As such, these devices are not generally exposed to the same level of interrogation of purpose that enterprise devices are regarding cybersecurity and the potential impact that they may have. To investigate this area, the sub-cases (A-C) presented in Figure 16 aim to capture the unique requirements of consumers.

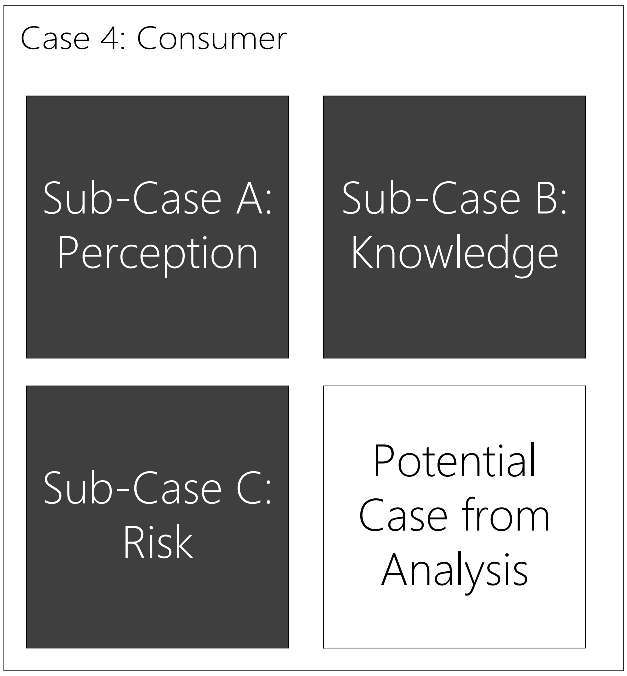


Figure 16: Case 4: Consumer Overview

3.3.7.4.1 Case 4, Sub-Case A: Perception

Consumers procure and view devices in a different light than enterprises or professionals. These differences in context create the potential for differences in how devices are marketed, deployed, and created. Such large differences also occur in regular markets – what is important is how it affects the application, adoptions, and usage of these devices. This perception also includes a consumer's knowledge of cybersecurity and the effect that knowledge has on IoT adoption or usage.

3.3.7.4.2 Case 4, Sub-Case B: Knowledge

This case aims to capture what constitutes an average level of knowledge and understanding for consumers. This includes aspects of IoT that may not be brought to consumer attention regarding privacy and security.

3.3.7.4.3 Case 4, Sub-Case C: Risk

In the same vein as risk in enterprise and cybersecurity, risk is still in consumer-grade IoT, however, it is less formalised. The impacts of this risk – including a consumer's acceptance, ignorance or calculation of risk must be identified, including any influence that marketing may have on these risk calculations.

3.3.7.5 *Case 5: Enterprise*

Enterprises are rapidly adopting IoT, and smart devices are commonplace, much the same as consumers. The adoption of IoT devices in an enterprise environment comes with the unknowns of any new technologies. When the benefits of these new devices exceed the potential risk from implementing potentially vulnerable devices and their associated workflows, which leads to early adoption. As each deployment and business is unique, the investigative areas depicted in Figure 17 will look broadly at overall business requirements instead of a specific business or organisation.

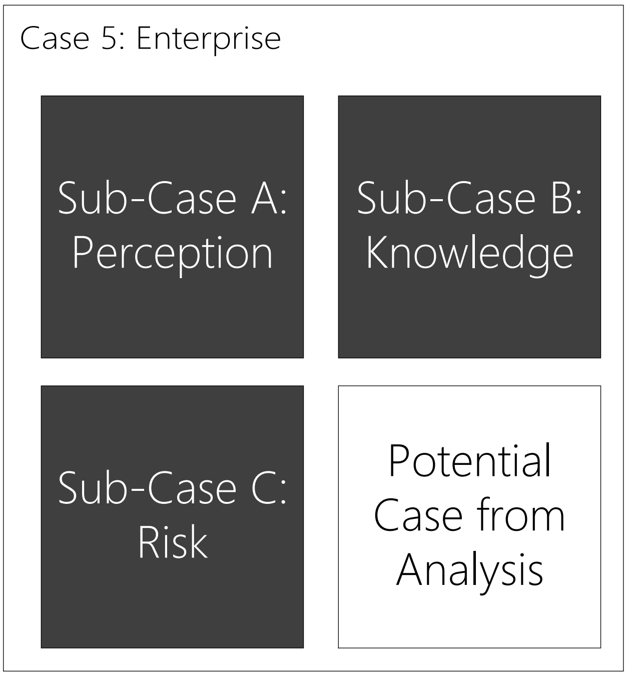


Figure 17: Case 5: Enterprise Overview

3.3.7.5.1 Case 5, Sub-Case A: Perception

Enterprises procure and view devices in a different light than consumers. These differences in context create the potential for differences in how devices are marketed, deployed, and created. Such a large differences also occur in normal markets – what is important is how is it affects the application, adoption, and usage of these devices. This perception also includes an enterprise’s knowledge of cybersecurity and the effect that knowledge has on IoT adoption or usage.

3.3.7.5.2 Case 5, Sub-Case B: Risk

Risk is well established in IT departments of enterprises. Given that IoT is a newer field, consideration must be given to how well is risk analysed by enterprises when evaluating IoT deployments, the subsequent impact of this analysis and the subsequent overall value proposition.

3.3.7.5.3 Case 5, Sub-Case C: Knowledge

This case aims to capture an understanding of IoT and what constitutes general knowledge for enterprises regarding IoT and its cybersecurity requirements.

3.3.7.6 *Design of Cross Analysis of Cases*

To aid in constructing such detailed and complicated cross-analysis, each case has been assigned a short-code, representative of their overall sequence in the research design. The short codes, detailed in Table 10 and Table 11, are used in the description and construction of the analysis plan.

Table 10: Case 4, Consumers Analysis Short-Codes

Case Identifier		Topic
4A	Case 4, Sub-Case A: Perception	Consumers: Perception
4B	Case 4, Sub-Case B: Knowledge	Consumers: Knowledge
4C	Case 4, Sub-Case C: Risk	Consumers: Risk

Table 11: Case 5, Enterprises Analysis Short-Codes

Case Identifier		Topic
5A	Case 5, Sub-Case A: Perception	Enterprises: Perception
5B	Case 5, Sub-Case B: Knowledge	Enterprises: Knowledge
5C	Case 5, Sub-Case C: Risk	Enterprises: Risk

3.3.7.6.1 Case 2, Consumer Case Cross-Analysis

The social impact for consumer of IoT is influenced by a myriad of drivers that are unique to consumerism. This case aims to gauge how consumers are affected by cybersecurity knowledge, expectations, and social influences. Table 12 shows the comparisons planned, a brief description and the expected outcome of each comparison.

Table 12: Case 2 to Case 4, Cross-Analysis Overview

Comparisons	Description	Expected Outcome
2 A,B,C to 4A	Take the devices, cybersecurity measures, networking and technical information and	An understanding of how technical knowledge of IoT will shape the consumers perception of IoT

(See Table 8 pg. 93 for Full Names of 2 A-C)	compare to a consumer's perception of IoT	
2 D,E,F,G to 4B (See Table 8 pg. 93 for Full Names of 2 D-G)	Take the cybersecurity regulations, risk and policy documents and analyse their impact on a consumer's knowledge of IoT	An understanding of how knowledge (or lack thereof) of regulation, risk, and policies impact consumers knowledge of IoT
2 A,B,C,D,E,F,G, to 4C (See Table 8 pg. 93 for Full Names of 2A-G)	Take the summation of cybersecurity principles in the IoT ecosystem from Case 2, and analysis how consumers understand risk for each of the different aspects	An understanding of how consumers understand risk for IoT overall, and how each aspect of is either calculations, accepted or ignored when interpreting risk

3.3.7.6.2 Case 2, Enterprise Case Cross-Analysis

Case 2, Cybersecurity Principles, requires application to be effective. As such, by taking the overall analysis from the cybersecurity case, we can apply them to the other prescribed investigation areas, looking for differences. Table 13 shows the comparisons planned, a brief description and the expected outcome of each comparison.

Table 13: Case 2 and Five, Cross-Analysis Overview

Comparisons	Description	Expected Outcome
2 A,B,C to 5A (See Table 8 pg. 93 for Full Names of 2 A-C)	Take the devices, cybersecurity measures, networking and technical information and compare to an enterprise's perception of IoT	An understanding of how technical knowledge of IoT will shape the enterprises perception of IoT
2 D,E,F,G to 5B (See Table 8 pg. 93 for Full Names of 2 D-G)	Take the cybersecurity regulations, risk and policy documents and analyse their impact on an enterprise's knowledge of IoT	An understanding of how knowledge (or lack thereof) of regulation, risk, and policies impact enterprises knowledge of IoT
2 A,B,C,D,E,F,G to 5C	Take the summation of cybersecurity principles in the IoT ecosystem from Case 2, and analysis how enterprises understand risk for each of the different aspects	An understanding of how enterprises understand risk for IoT overall, and how each aspect is of each is calculated, accepted, or ignored when interpreting risk

3.3.7.6.3 Overall Cross Analysis

Whilst the embedded case studies are critical to performing a deep dive into a smaller segment of the whole, we must also be able to analyse the bigger picture between macro systems. By taking the embedded case studies and distilling the core outcomes of each, they can be combined into larger picture for a broader analysis. This is shown in Table 14.

Table 14: Overall Case to Case Analysis Overview

Comparisons	Description	Expected Outcome
2 to 4	Take the entire case of cybersecurity principles (case 2) and compare it to the entire case 4, consumer Socioeconomic Impact	An overall understanding of how cybersecurity principles relate to impact consumer Socioeconomic Impact, and vice-versa
2 to 5	Take the entire case of cybersecurity principles (case 2) and compare it to the entire case 5, enterprise Socioeconomic Impact	An overall understanding of how cybersecurity principles relate to impact enterprise Socioeconomic Impact, and vice-versa
4 to 5	Take the entirety of case 4, consumer Socioeconomic Impact and compare it to case 5, enterprise Socioeconomic Impact	An understanding of overall differences between consumer and enterprise concerning IoT

4 Case 1: IoT Networks and Systems

This case is designed to investigate and identify the boundaries of the IoT ecosystem. IoT has a basic definition, given by the Merriam-Webster Dictionary as "the networking capability that allows information to be sent to and received from objects and devices (such as fixtures and kitchen appliances) using the Internet" (Merriam-Webster, n.d.). Whilst this is a serviceable definition for identification of the concept of IoT, the broadness of this definition creates an issue when attempting to identify details within IoT and its subsets.

The analysis of the language contained within this case is not attempting to debate what IoT is, or if the language used is correct. Instead, the focus is on discovering what is currently in active use to describe the areas that can be ascertained from the application of IoT for different outcomes. A key output of this case is the supplementation of existing definitions and using these definitions to both identify and limit the investigative area.

4.1 Contextual Notes

The contextual view for this case can be described as pragmatic. The aim is to identity the logical aspects and not on the wider usage or adoption of IoT.

4.2 Case Specific Inputs

This case is concerned with the creation of research scope boundaries; as such, the research inputs are substantially different to subsequent cases. The contextual inputs for this case are the researcher's contextual knowledge of IoT, cybersecurity, networks, and the information discovered during the literature review – which is also an aspect of the contextual knowledge of the researcher.

4.3 Intended Case Outputs

This case aims to produce of a series of logical areas that can be used as bounding boxes for later cases. The following lists prescribes the expected outcomes of this case:

- The Identification of:
    - IoT as a concept
    - Existing IoT Definitions

    - Common Characteristics of IoT
- A grouping of IoT terminology
- Creation of logical IoT categories

Using the resulting IoT categories, further cases can have clearer constraints with which to investigate the ecosystem of IoT. Without these clearer constraints to aid in defining the investigative areas of the research, there is a significant possibility that the investigation would be too broadly scoped due to an overly large investigative area.

4.4 Case Location in the Research Design

Figure 18 denotes the current case's location in the overall research design. This case, (Case 1) is the first of the cases of the overall research method and sets the areas that will be investigated in more detail.

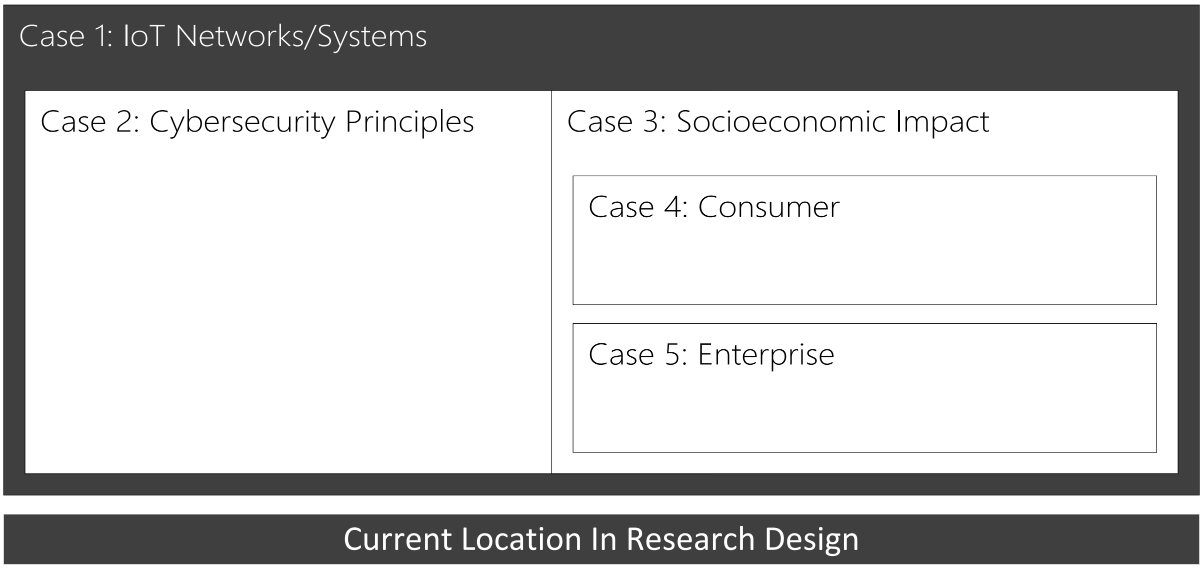

Case 1: IoT Networks/Systems
Case 2: Cybersecurity Principles
Case 3: Socioeconomic Impact
Case 4: Consumer
Case 5: Enterprise
Current Location In Research Design

Figure 18: Current Case Location in Overall Research Design

4.5 Case Content

This case aims to answer the following research questions:

- How do we define the term Internet of Things (IoT)?
- It is possible to create a categorisation schema for IoT?
    - How do we define the term 'Healthcare Internet of Things' (HIoT)?

In answering the first question of 'How do we define the term Internet of Things (IoT)', firstly the current definition must be shown to either be acceptable or deficient. As previously mentioned, a current definition of IoT is "the networking capability that allows information to be sent to and received from objects and devices (such as fixtures and kitchen appliances) using the Internet" (Merriam-Webster, n.d.). This definition is acceptable for a broad and conceptual level understanding of IoT.

However, this conceptual definition is not specific enough, as the application of IoT changes radically depending on the context of the applied IoT devices and their associated systems. This different application per deployment means that the tangible reference of IoT becomes difficult to discern. In addition, it also means that any attempt to capture IoT at a granular level is highly difficult, verging on impossible due to the adaptive and adynamic nature of the field.

To address the need to identify IoT in all areas, we do not need a new definition, but a way of classifying IoT across any common characteristics, agnostic of devices. Before such a device-agnostic categorisation system can be created, the terms and language used to describe the IoT field must be analysed, to capture the common points that can then be built on. The following steps of linguistic analysis of devised via critical analysis of the problem at hand – how to investigate the language of IoT:

1.) Ascertain the existing terminology and constructs
2.) Analyse IoT terminology to extract common categories
3.) Group by device characteristics or application type
4.) Using these groups and characteristics, extract any common characteristics that may help define the IoT Ecosystem

The identification and analysis of the diverse language used in the IoT was required before Case 1 could commence in full. This analysis nominally forms part of the case itself and is contained within the content of Case 1.

Most of the terms describe a specific concept within IoT and not an individual device's capabilities. As the terms are targeted at a conceptual level, attempting categorization based on devices would create needless work and run contrary to the goals of this case. Such a device-specific approach would also be more rigid and would exacerbate the already identified issues of fracturing and disparate language by potentially injecting more language and terms to account for this specificity.

4.5.1 Terminology

The usage of language in everyday life is both intrinsic and complicated. When interpreting language, we perform many processes automatically and in parallel to interpret the meaning of words, phrases, and other linguistic constructs. The study of language is extensive; however, the application of the theory presented to the issue of IoT terminology is the goal of this chapter - not a comprehensive presentation on the philosophy of language. As such, in agreement with McGinn (2015) the study of language can be said to be "*…concerned with the general nature of meaning*". It is this general prospect of meaning and subsequent understanding that highlights the issues present within IoT.

When applied to research and development, the generalisation of meaning becomes a challenge - more so in quickly advancing theories and heavily researched fields, such as IoT. This challenge manifests itself as a multitude of new terms to describe the rapidly evolving field, of which a coherent definition does not exist. This language barrier is of particular interest in IoT, as this concept spans many research fields with differing interpretations, contexts, and ideas, compounded further by the 'acronym soup' that is already present in the ICT industry.

This problem of language is exacerbated by the shortening of terms to acronyms, and is not a new issue (Thilmany, 2003). This occurs across all facets of IoT, with manufacturers, engineers, and scientists all having the same issue – identifying the acronyms and their associated meaning.

This identification process can be explained by taking the philosophy of language and analysing how meaning and context are used in understanding acronyms. This is made more difficult by the lack of a framework and common reference point to begin the arduous task of defining these terms.

4.5.2 Language and Context

The study of language is an old, well established, and multifaceted research field. Language is not static as a tool; it evolves; words shift in context, meaning, interpretation, and understanding. This movement shapes how we utilise language to interpret the world, and to communicate ideas and concepts. The following analysis involves several keywords, which the English language has multiple meanings for. When *italicised*, these words are to be taken as the concept that will be associated with them, and not the word as written. It should be noted that where there is an interpretation of terms, that the interpretation is informed by the process detailed this section (4.5.2) and informed by extensive cybersecurity knowledge and experience.

We must first describe how we interpret language and what logical segments language contains. This discussion is not a comprehensive presentation of linguistic construction and instead focuses on applying theory and concepts to an analysis. This analysis forms the foundations of an argument and begins with Frege's *On Sense and Reference* (Frege, 1948). There are more modern interpretations that present the same overall viewpoints, for example *History of English* (Culpeper, 2015) and *Philosophy of Language: The Classics Explained* (McGinn, 2015).

This continued refinement and development of the philosophy of language means that only some of the ideas presented by Frege (1948) have survived scrutiny or modern changes to interpretation. To analyse the terminology of IoT, we are concerned with how Frege (1948) structures *sentences* and *propositions*, as well as their constituent *components*.

In understanding the construction of a *sentence*, the core relevant concept is that of a *sign*. As explained by McGinn (2015), this relates to a *proposition* – when constructing a sentence, you are also constructing a *proposition* of something. This means that it is entirely possible and quite common that two completely different sentences can have the same *proposition*.

This construction applies within a languages' dialects, and as a demonstration of this principle, take the following example:

- Amy is single.
- Amy is a bachelorette.

Both put forward the same *proposition* – the terms single and bachelorette, in this case, are synonymous and are taken as having the same meaning. Whilst social identifiers will change this synonymous meaning depending on who is spoken to, for this case, it is enough that one of the possible *propositions* is identical. As a further example, the same can be demonstrated across language boundaries, between English and Italian:

- Blood is red.
- Il sangue è rosso.

Whilst the two sentences are entirely different, they still express the same *proposition*. This construction of two sentences making the same point is critical to the analysis of the language of IoT – where the technology mix fits the colloquial 'melting pot'. Whilst this point of agreement is critical, the process of interpretation and understanding of how we arrive at this proposition is crucial to the analysis of any terminology within IoT.

There are four steps to this understanding and interpretation, taken from Frege (1948), who is sometimes called the "Father of Modern Philosophy" (Culpeper, 2015; McGinn, 2015). When taken together, these steps demonstrate the process of interpreting a sentence. In order, these steps are:

1.) Components
2.) Context
3.) Sense
4.) Reference

Beginning with *components*, they are influenced by the concept of a *sign* presented by Frege (Frege, 1948). The core concept of a *sign* can be presented as a 'constituent part' or an 'individual thing' that can be logically separated and identified. This concept is not a major point of contention; however, differing interpretations exist with the field of philosophy of language – a discussion of which is out of the scope of this research. This first step (the identification the individual parts) allows for the next step in the process - *context*.

Context is the stage where a person, as an individual, applies their contextual knowledge when attempting to understand the presented components. This contextual knowledge will shape the later stages (*sense* and *reference*) and is performed simultaneously as the *components* are identified. This simultaneous interpretation can be demonstrated using the following phrase:

- "The Prime Minister of Australia"

Applying the first two stages (*components* and *context*), we first identify the individual *components* – "Prime", "Minister", and "Australia", and then the compound *components* of "The Prime Minister" and "of Australia". Grammatically, they are different, and this process has abstracted away the process of understanding the language, and the characteristics of different language constructs and their impact on semantics.

Without context, these *components* do not hold any knowledge, nor are they signifying a proposition – they are simply logical separators for us to compartmentalise and begin to apply *context.* It is sufficient that each component can be identified as a standalone logical entity without understanding what that abstract entity is. This identification of elements is crucial to the eventual reference and understanding of the presented sentence.

Given that we now know of three separate components, the next phase, *context*, begins. Logically, this is a separate process; however as stated, when interpreting a sentence, it is performed in parallel with the identification of *components*. This process applies background knowledge, personal beliefs and personal interpretation that is unique to each person. This phase is where knowledge from different fields of study will influence the next phase – *sense*.

Sense is a logically separated component of the sentence structure, except when interpreting a sentence. This is a parallel and intuitive process that is intrinsically linked to the *components* and *context*. The application of *context* and *component(s)* draws on an individual's understanding and knowledge base to formulate an understanding and draw the *sense* of the separate logical entities. In essence, coming to a *sense* is the base understanding of the *proposition.* In deducing the *sense* of a *proposition*, the *context* for each person will be unique, and without agreed-on definitions of terms, multiple interpretations will occur. As IoT is a multi-disciplinary concept, the problem of *sense* becomes less clear because of the unique context that each person brings to the interpretation of the *proposition*. Attempting to reach common ground and understanding, having a multitude of unanchored interpretations is difficult – especially when attempting to apply cybersecurity to any system, as common definitions and clear understandings are paramount.

These contextual and interpretational differences are highlighted when attempting to interpret a *sense*. To take an example to illustrate this, we say the following:

- "The 101st Prime Minister of Australia"

This statement makes perfect *sense* – nothing is blocking us from making a comparison, utilising contextual knowledge to conjure up an image of a Prime Minister of Australia, who is the 101st in office. This statement, whilst making perfect *sense*, is not attached to a *reference*. This lack of a reference is not demonstrated in following statement:

- "The current Prime Minister of Australia"

This statement again makes perfect *sense* – nothing is stopping the identification of *components* and the application of *context*, which, when taken together, present a *sense* of a Prime Minister of Australia. The difference is that this *sense* also can be followed onto the final step - a *reference*.

A *reference* takes our intuitive separation of the logical items presented (*sign)*, applies our contextual knowledge (*context*) to form a picture of the *proposition*, and then attempts to make *sense* of the interpretation by attaching it to a known entity. This attachment to a known and defined entity is required for a *reference*. It is important to note that an entity need not be a physical thing – it may be an idea or a concept that is clearly defined and understood. Using this example, the *reference* would be a person, who at the time of reading the phrase, is currently appointed at the Prime Minister of Australia.

When applying this simplified linguistic analysis to an actively researched and developed industry field like IoT, the overlap between multiple fields and contextual knowledge bases causes different terms to be coined in language. These terms may have a single *proposition* for the application of an idea within IoT; however, due to the rapid and disparate development, many terms have appeared to describe the same *reference*. This multiplicity means that identification of the different techniques, devices and technologies is hampered by many differing names, phrases and acronyms when searching for information.

4.5.2.1 *Interpreting IoT*

As a result of the above multiplicity, there is a lack of clear distinction within IoT, and there is no agreed-on mapping of terms-to-function. Using Frege's analysis, each major term is analysed to ascertain its four aspects: *components*, *context*, *sense*, and *reference*. This analysis will allow for the identification of which terms refer to the same *reference* and any similarities. Where identified, should two disparate terms resolve to a shared *reference*, they can be said to making the same *proposition* and thus, identical.

This analysis will allow for the categorisation and analyse of the IoT ecosystem based on their common *sense* and *references*. To illustrate the long form and demonstrate the process of the linguistic breakdown, we can use the umbrella term 'The Internet of Things', shown in Figure 19.

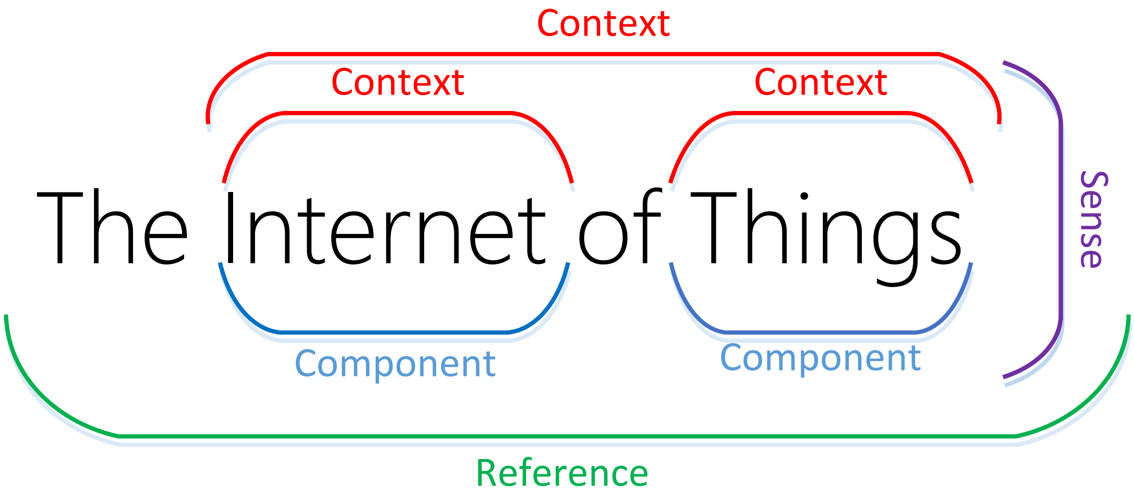


Figure 19: Internet of Things, Language Interpretation

4.5.2.1.1 Process to understanding

Starting with the *components*, we have both "internet" and "things". Without any *context*, we do not yet attach these to any known item or concept. Instead, they are the logical separators that identify the different segments that contain contextual knowledge. This contextual knowledge will differ from person to person. By applying *context*, we can ascertain that the internet is a worldwide communications network, and things are small, low powered devices. As "things" for the "internet" are ambiguous and can vary greatly depending on individual *context*.

In essence, this means that the *sense* conjured by a person in the medical field will differ greatly from the *sense* envisioned by a software engineer. This comes about from a myriad of factors, including their existing knowledge, viewpoints, technological understanding, and overall interpretation of terms. To resolve this, we must ignore a measure of the individual *context*, moving away from individual specifics and focussing on the overall *sense*. This is done by widening the *context*, and creates a more generic *sense* that is widely applicable – establishing an overarching *sense* of IoT; the concept of small low powered devices, that can communicate using the internet.

To move from a *sense* to a *reference*, the concept that the *sense* describes must be attached to a tangible thing – only once the *sense* becomes, in essence, 'real' does it becomes a *reference*. This tangibility requirement is not limited to physical objects – a clearly defined and understood concept can also be a *reference*. To illustrate the difficulty in applying this to IoT, the *sense* that is presented – "small low powered devices, that can communicate using the internet" follows the expected process and becomes a direct *reference* to IoT. However, there is a duality for IoT – as there is more than one *sense*, so there is more than one *reference*. In this case, there is IoT the device, and IoT the concept. In this example, the device and concept remain in agreement.

This agreement is not guaranteed, as *context* differs for each person and research area, generating different interpretations, and subsequent differing language and terminology. It is this process that has given rise to the myriad of terminology to describe the same concepts within IoT.

4.5.2.1.2 Issues in Interpretation of IoT as a Proposition

As the technology and application of ideas within IoT are bleeding-edge, the rapid development of the devices will adhere to the *sense* of IoT, with the differences in *context* feeding the creation of new terms to address these differences. However, these terms will still address the same *reference*. This general process is the core issue with the language used within the IoT ecosystem and is further exacerbated by the rapid, leading-edge research and development that causes further evolution of terms – the creation, testing and adoption or discarding of new terms to suit the *context* of IoT under development.

It is not the aim of this research to ascertain the relationships between the evolution of language and the evolution of devices and the influences therein, instead it is to ascertain how we can understand the evolving issues that this presents specifically in relation to cybersecurity.

Primarily, there is a disconnection between the usage of new terms to describe applications of the concept of IoT, the developed devices, and the concept of IoT. This disconnect results in a non-cohesive ecosystem of disparate devices, protocols, and systems, which represents itself in the multiple terms used to describe parts of IoT. An example of this is the set of terms Cyber-Physical Systems, Industrial Internet of Things, and Internet of Industrial Things. This comes about partly due to the flexible nature of IoT as a computing concept where a device is not always a physical device – it may be a piece of software or a segment of a larger whole.

This flexible ecosystem is beneficial and problematic – beneficial that solutions are not constrained to one instance, and problematic that different deployment instances have their own terms, definitions, and applied contextual knowledge. The added complexity comes from technical terms within specialised areas, and the saturation of terminology across all both technical and non-technical communication. This creates an area where coming to a *reference* from differing terms is substantially more difficult.

Specific terminology exists within every field, and are, for the most part, different enough that the problem described does not arise. As an example, Quantum Computing has the term *Hadamard Gate*, but no such similar term exists with the field of IoT. However, the increasing digitisation of most aspects of life, the crossover of terms and re-use of similar or same terms with a different meaning now occurs more often. The inverse also occurs, where there are a multitude of terms used to describe the same *reference* – it is this aspect that IoT suffers from the most.

4.5.2.1.3 Example Breakdown of the Term IoT

As presented in Figure 19, IoT is both a complicated and straightforward breakdown of terms, as it *references* both an idea and thing. Reiterating the process (from 4.5.2.1.1) the first step is to break this apart into the *components* – an "Internet" and "Things". Applying the *contextual* knowledge from a cybersecurity perspective, the terms can be expanded to identify that the "Internet" is a "worldwide communications network", and that "things" are "small, low powered devices communicating using a network". This interpretation only holds true when, contextually, we are talking about a *device*. This chain of interpretation is not always true, as there are multiple possible *senses* when interpreting IoT.

One interpretation is the identification of the broader *sense* of IoT - "Anything, networked together to form a system, that may make autonomous intelligent decisions". Another is the concept of "computing devices performing intelligent actions", where the *device* is a physical *thing* and not part of a perceived idea. The concept can be presented as an umbrella term – encapsulating the application of the different *senses* across the multitude of different computing systems.

The historical interpretation of IoT concepts plays a role when applying *context*. Understanding a previous version of the concept and the subsequent changes to the concept will shape contextual understanding and consequently the eventual interpretation – this is congruent with the application of *context* as described in 4.5.2. This contextual shift is prevalent in systems of systems – as software and computing become more intrinsically linked with the advent of cloud and other computing services – like serverless architecture, the "thing" aspect of IoT can now be decoupled from the physical device.

This decoupling causes further issues as the identification of system boundaries becomes more difficult to identify, as devices lose some of their tangibility of association to a physical thing, instead relating to a concept. This abstraction also causes additional interpretation, as an extra step is now required to identify the physical “thing”. This abstraction of context can occur at multiple levels, and each time it occurs it creates additional difficulty in establishing the *reference* of a given “thing”.

The analysis of each major term identified, utilising the method described in section 4.5.2, will break apart each of the terms to identify their final *reference*. This breakdown allows for a more detailed analysis of the terms along with both their unique and overlapping characteristics. The following terms were identified during the process of the literature review. The Internet of Things is presented as an umbrella term, with Cyber-Physical Systems (CPS) and Healthcare Internet of Things (HIoT) residing as applications of IoT to a specific area. Finally, other derived terms sit under CPS and HIOT respectively. This is shown in Table 15.

Table 15: Major IoT Terminology

Internet of Things (IoT)	
Cyber-Physical Systems (CPS)	Healthcare Internet of Things (HIoT)
Smart Cities Ubiquitous Computing Industrial Internet of Things (IIoT)	Internet of Medical Things (IoMT) Internet of Healthy Things (IoHT)
	Satellite Terms
	M-Health (mHealth) Tele-Health E-Health (eHealth) Health 2.0

The following analysis is split into two segments to address the two distinct applications. Firstly, the terms that are outside of any medical association are analysed. Subsequently, any terms that are associated with medical field are then analysis. This deliberate split is to account for the unique context and addition rigour comes with medical terminology. As *context* is the main factor that shapes all analysis, the overall *context* for every analysis of a term must be stated. In this case the context for all analysis is that of the individual researcher performing the analysis.

4.5.2.1.4 Non-Medical Terminology

As presented in Frege's theory (4.5.2) (1948), there are four aspects of interpretation - *components*, *context*, *sense*, and *reference*. Each section below will be structured following in the following way: first the identification of *components* and *context*, the identification of the *sense(s)*, and then the *reference*.

IoT is a difficult term, as it holds multiple *senses* and *references* within the same term, heavily dependent on *context*. For this research is sufficient that the split in concept versus device can be identified. The set of analyses will examine IoT, IIoT, CPS, Smart Cities and Ubiquitous Computing and their interrelations.

4.5.2.1.4.1 Cyber-Physical Systems (CPS)

Presented in Figure 21, Cyber-Physical Systems are not immediately relatable to IoT but after interpretation become nearly identical in scope to IIoT. The two components – "Cyber-Physical" and "Systems" are abstracted and rely heavily on context to come to a *sense* and a *reference*. This contextual understanding is needed to identify that "Cyber-Physical" is the interplay of digital devices that interact with the physical world and that the "Systems" are some form or segment of an ICT system. The *sense* derived from this is similar, if somewhat broader in scope to IIoT – "the application of smart devices that perform physical interactions with the world, created from multiple interlinking systems".

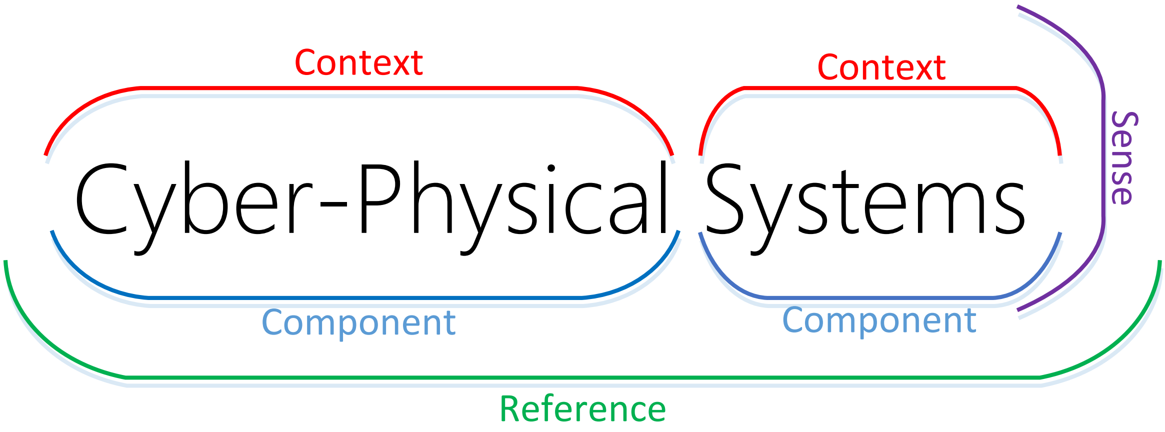


Figure 21: Cyber Physical Systems: Component, Context, Sense & Reference

This attaches to the *reference* to both a physical device as part of the system and the concept of the system itself. Whilst it potentially possible to argue over semantics, the usage of CPS and IIoT can be used interchangeably, as they both, conceptually, deal with the same areas – applying the IoT paradigm to the problem of physical integration and control from a digital system.

4.5.2.1.4.2 The Industrial Internet of Things (IIoT)

Presented in Figure 20, The Industrial Internet of Things is the application of the IoT conceptual *sense* to industrial systems. This application aims to supplement or replace existing Supervisory Control and Data Acquisition (SCADA) Systems or the broader scoped Industrial Control Systems (ICS).

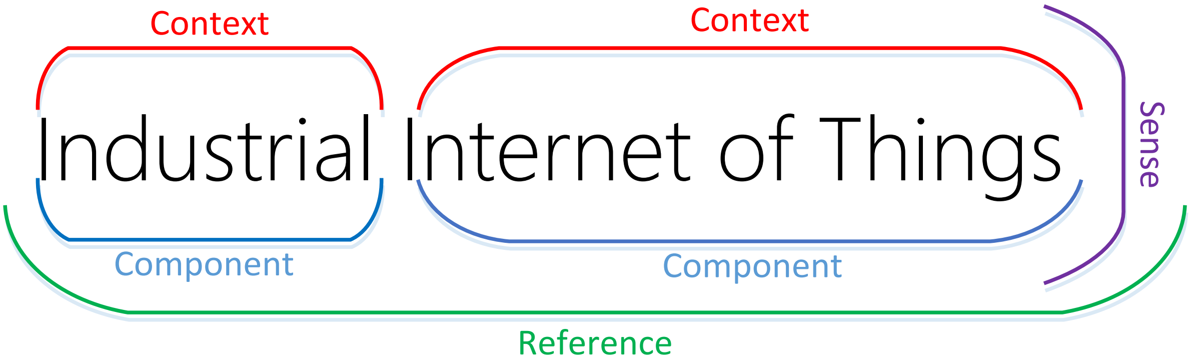


Figure 20: Industrial Internet of Things: Component, Context, Sense & Reference

Breaking apart the phrase into *components*, we are left with ‘industrial’ and ‘internet of things’. Contextually, IIoT suffers from the issues presented by IoT, and the differences in *context* that occur due to the broad scope of ‘industrial’. Applying *context*, ‘industrial’ can be related to the SCADA systems and their interoperability, or large-scale manufacturing or other industrial processes. IoT has the same interpretation as presented in 4.5.2.1 ‘Interpreting IoT’, as it is an inherited interpretation.

The *sense* of IIoT is similar to IoT in that it inherits the multiple *sense* and *reference* issues of IoT. As IIoT is an application of IoT, these inherited issues are magnified by the additional layer of *context*. As such, the *context* of IoT, in this case, must be mixed or layered to take account of the specific applications within the field of operation, ‘industrial’. This industrial *context* contains nuances and can relate to anything from automation in a factory to controlling a dam’s sluice gates.

This wide encompassment results in a *reference* that can be both physical and conceptual. As such, the physical *reference* will be to the devices themselves (inheriting the decoupling issue from IoT), and the conceptual *reference(s)* can apply to the *sense* of “an industrial system, using both IoT devices and the computing approach of IoT”.

4.5.2.1.4.3 Smart Cities

As shown in Figure 22, Smart Cities are the application of IoT to all aspects of a cities' services. Breaking apart the phrase into *components*, we obtain 'Smart' and 'City'. Both are universal terms and rely heavily on the *context* to draw any further understanding. *Contextually*, the component 'Smart' inherits the namesake of the IoT 'smart' – the small, low power devices that can act with intelligence. The 'Cities' component is only slightly modified from the initial overall 'urban' view of a city and is readjusted to the services that run a city - with the addition of the 'smart' devices into this already existing system of systems present within a modern city. This results in the *sense* of a distributed, connected, and autonomous decision-making city. This *sense* coincides somewhat with the phrase Cyber-Physical Systems, as they are both concerned with systems that are creating physical interactions via digital means.

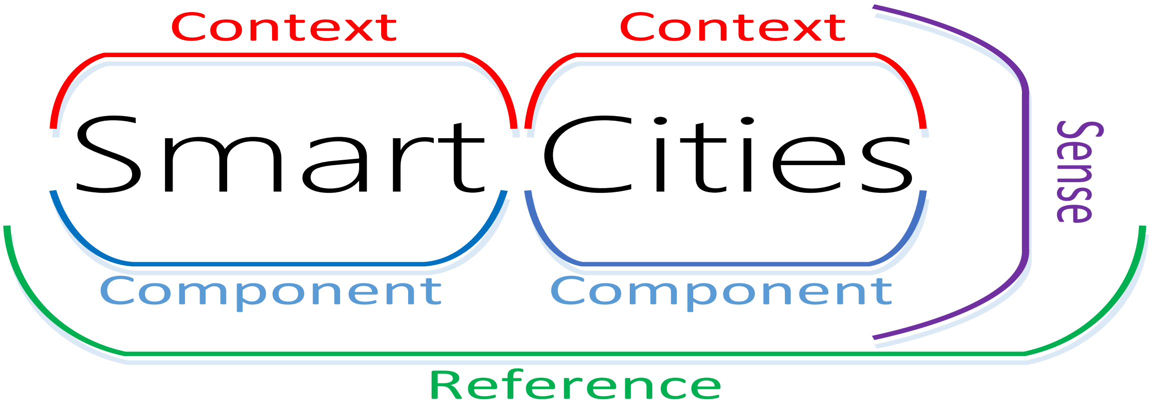


Figure 22: Smart Cities: Component, Context, Sense & Reference

4.5.2.1.4.4 Ubiquitous Computing

This discussion around IoT and it relation to the topic of Ubiquitous Compuing (UQ) not new, and has been a point of discussion and research for some time (Weiser, 1993). It can be construed that UQ is simply the forefather of IoT; however, this runs the risk of conflating the two distinct concepts. IoT is focused on devices and their interactions, driven by data (Atzori et al., 2010). UQ is focused on the invisibility of devices, and this difference results in very different outlooks (Lyytinen & Yoo, 2002). As such, while both UQ and IoT may influence one another, UQ has arguably been around longer and stands as a distinct concept that is different from IoT.

As shown in Figure 23 the *components* given are Ubiquitous and Computing. In difference to previous terms (IIoT/IoT), these terms do not rely as heavily on *context* to facilitate understanding.

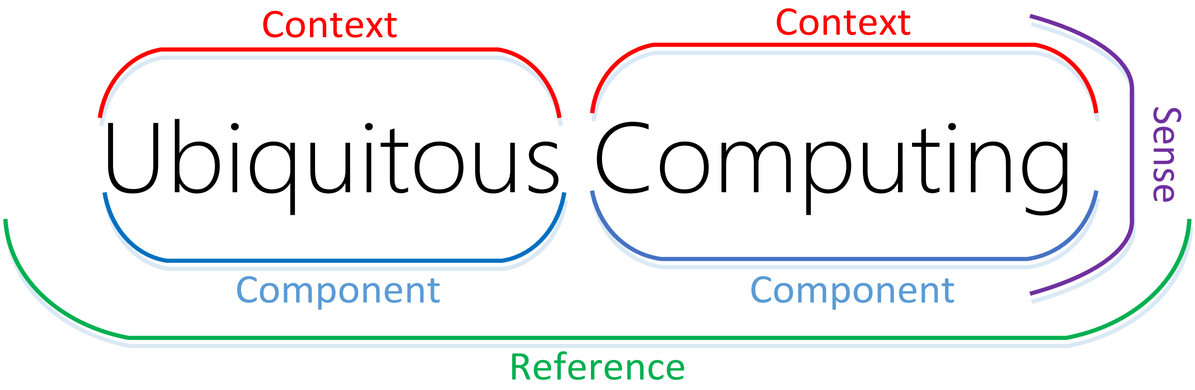


Figure 23: Ubiquitous Computing: Component, Context, Sense & Reference

Given *context*, the terms are interpreted as is, with little 'outside' information required, given that the *components* definition in common language aligns with the *sense* of Ubiquitous Computing.

This concept will shift with *contextual* knowledge of computing devices and their capabilities; this does not change the overall interpretation, merely a single aspect of it. This *sense* can be described as 'the non-intrusive availability of computing power, almost (if not entirely) invisible to the user'. This term, however, still suffers from the multiple *sense-reference* issues that are prevalent within IoT, as a *reference* could refer to both the concept and the devices used to describe the concept.

4.5.2.1.5 Medical Terminology

When dealing with medical terminology and IoT, a differing set of contextual knowledge applies. Medical terminology is highly complex, well established, and clearly defined with less flexibility in terminology overall. This is in contrast to the highly dynamic terminology used with ICT. This overlap of clear, structured, and agreed-on language versus a fluid, dynamic and rapidly evolving terminology creates an additional layer of comprehension that must be navigated. This collision of disparate industries and associated terminology is not a new phenomenon, as all multidisciplinary systems will have some form of term collision necessitating a clarification between the communicating parties.

Due to this potentially large difference between terms, the *context* and subsequent interpretation of terms like IoT by medical professionals will differ greatly from ICT professionals. This difference of interpretation is true for all professions (and people); however, it is greatly magnified given the complexity that is present within medical *contexts*. As there is now an additional layer of *context* (the medical application), the interpretation and understanding becomes more difficult.

4.5.2.1.5.1 Internet of Medical Things

As shown in Figure 24, The Internet of Medical Things (IoMT), when split into *components* contains three aspects 'Internet', 'Medical' and 'Things'. *Contextually*, the 'Internet' aligns with its definition and may partially inherit from the Internet in IoT due to the 'Things' component and the comparative *context* the similar terminology creates. 'Medical' has a broad scope of interpretation, covering both clinical and non-clinical applications, and 'Things' is drawn directly from the 'Things' of IoT.

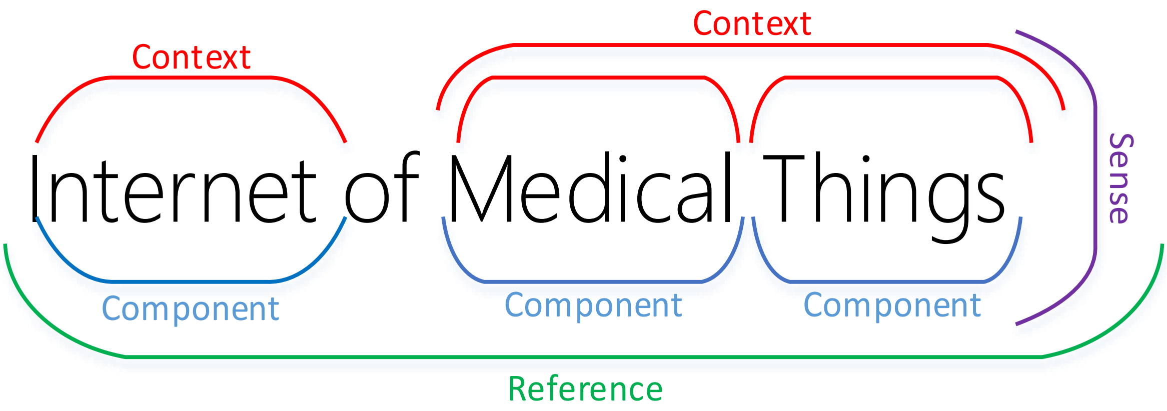


Figure 24: Internet of Medical Things: Component, Context, Sense & Reference

Medical 'things' is the broadest layer, as without identifying the larger aspects first, specifics become impossible to identify. This is demonstrated in Figure 24 by the larger *contextual* line, covering both 'medical' and 'things'. The two-layered interpretation is used in all aspects of IoT medical terminology, as each requires that each *component's context* is clearly identified, then further knowledge is drawn from the broader *context*.

This results in a *sense* of 'A collection medical devices and applications that utilise IoT to provide healthcare solutions'. As this *sense* relies on IoT to draw its conclusion, all the issues that are present in IoT are also inherited by IoMT. This includes the multiple *sense-refere*nce issues within IoT, albeit with respect to the medical *context*.

4.5.2.1.5.2 Healthcare Internet of Things

As shown in Figure 25, The Healthcare Internet of Things (HIoT) is similar to the IoMT, with some nuanced differences. The *components* provide us with 'healthcare', 'internet', and 'things'. When interpreting the broad, 'outer' layer of *context*, the interpretation of 'healthcare' can be either health, wellness, and wellbeing or from a clinical perspective, would include medical application such as treatment and diagnosis. This split interpretation is contrary to IoMT, as 'medical' shares the single, clinical *sense*.

The rest of the *context* is a mirror image of IoMT, with IoT the source of inherited *context* and the subsequent issues. The second layer and the focus on more informal and non-clinical devices means that the implications of 'clinical usage' is the secondary *sense*, with the main aspect being the non-clinical, consumer self-lead application.

As such, the *sense* is also the mirror of IoMT – "A collection medical devices and applications that utilise IoT to provide healthcare solutions". This results in a *reference* that ranges from healthcare wearables, like fitness trackers, to monitoring system in a home or assisted living environment.

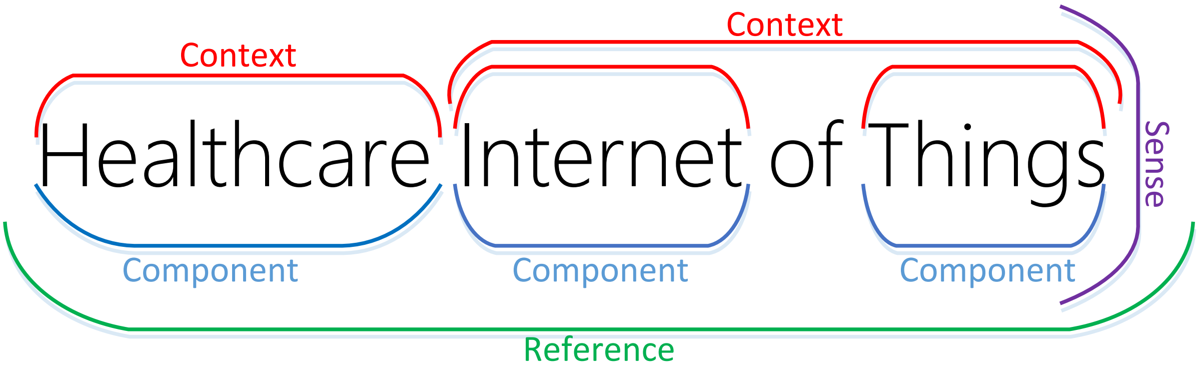


Figure 25: Healthcare Internet of Things: Component, Context, Sense & Reference

4.5.2.1.5.3 Internet of Healthy Things

Shown in Figure 26, the Internet of Healthy Things is closer to HIoT than IoMT. The *components* are 'internet', 'healthy' and 'things'. In respect to IoMT and HIoT, both 'internet' and 'things' have the same *contextual* interpretations. The 'healthy' *context* is more abstract and will be shaped by the reader, however the *sense* of 'an internet containing things that make a person healthy' when interpreted from a personal *context*.

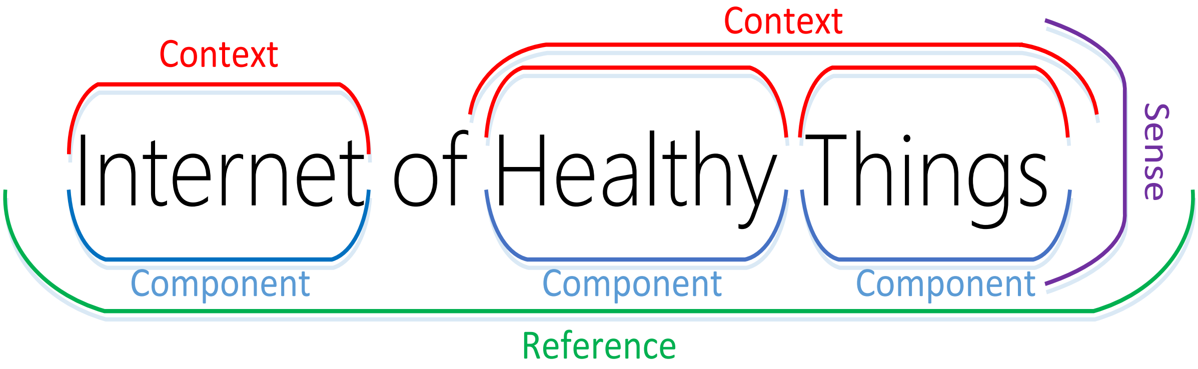


Figure 26: Internet of Health Things: Component, Context, Sense & Reference

Alternatively, more abstractly, 'An internet of things that contains health providing things'. Whilst these *senses* are written differently to IoMT or HIoT; they are, when resolved to their *reference*, referring to the same core idea – IoT applied to a healthcare *context*.

4.5.2.1.5.4 Satellite Terms

The following terms are deemed satellite terms. They have a minimal direct impact and are only partially included or influenced by the technologies. However, they did appear in terminology searches and incorporated some of the aspects of IoT and HIoT into their own distinct fields. The terms are included for completeness, however, bear little to no impact on the overall research. Due to their limited impact, a full linguistic analysis was not performed.

4.5.2.1.5.4.1 M-Health

Mobile Health (mHealth, M-Health) is the application of mobile devices (phones, PDA's etc.) to the delivery of healthcare services. It can be included as a sub-set of E-Health.

4.5.2.1.5.4.2 Tele-Health

Telehealth is generally defined as the "use of telecommunication techniques to provide telemedicine, medical education, and health education over a distance" (White et al., 2001).

4.5.2.1.5.4.3 E-Health (eHealth)

There are arguments as to the scope of this definition, with two main aspects (Eysenbach, 2001). One, broad, to encompass the usage of electronic and digital processes in healthcare. The other is narrow and is defined as the usage of healthcare practice using the internet.

4.5.2.1.5.4.4 Health 2.0

Health 2.0 is less of a defined aspect of healthcare and describes the advancement and change of healthcare to incorporate the demands of modern society and technologies (Van De Belt et al., 2010). There are similar terms to describe a technological uplift and change of approach – Industry 4.0, Internet 2.0 and are generally used to denote a milestone and advancement at a conceptual level.

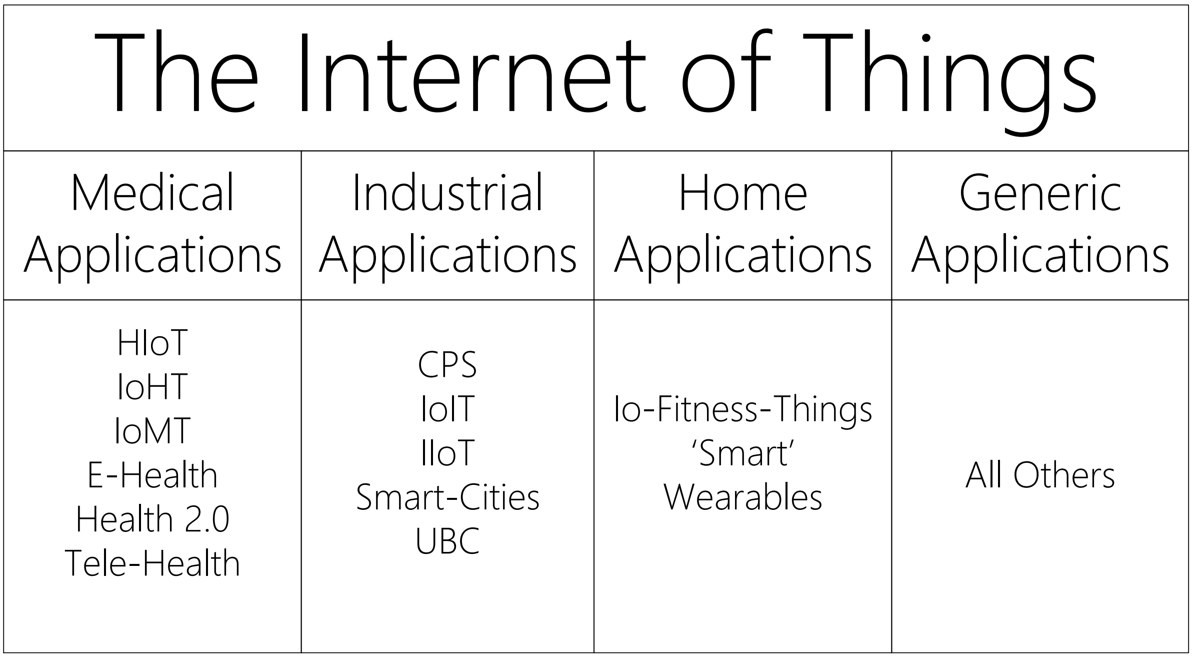
4.5.3 Categorising IoT

Using the context from the language analysis, a modicum of the existing ecosystem can be maintained to draw the current terms together, instead of attempting to reinvent a classification schema. Whilst this is seemingly contrary to the need to avoid device level specifics, there is agreement on the broad concepts and general characteristics of an IoT device that avoids the previously mentioned faults.

The device characteristics include:

- That devices are usually physically small and low (or battery) powered
- Can be a part of a geospatially dispersed deployment
- May have periods of sleep where the device is in a passive or sleep mode
- The device will not always be actively sending or receiving data
- Contains at least one sensor of some description (usually multiple)
    - These sensors measure some sort of physical phenomena
- May communicate with non-TCP/IP compatible protocols

Thus, the following four categories are (Figure 27) are used to guide the segmentation of IoT into smaller, logical bounding boxes that can be analysed according to their contextual requirements. The listed items within Figure 27 are used only as examples – not all terms are discussed further.



<table>
<tr><th colspan="4">The Internet of Things</th></tr>
<tr><th>Medical Applications</th><th>Industrial Applications</th><th>Home Applications</th><th>Generic Applications</th></tr>
<tr><td>HIoT
IoHT
IoMT
E-Health
Health 2.0
Tele-Health</td><td>CPS
IoIT
IIoT
Smart-Cities
UBC</td><td>Io-Fitness-Things
‘Smart’
Wearables</td><td>All Others</td></tr>
</table>

Figure 27: IoT Categorisation Schema

The four categories allow for the identification of IoT devices by application and characteristics. This usage-based categorisation also allows for easier application of contextual aspects, as ‘bleed over’ from conflicting or irrelevant areas is minimized.

These broad categories can be further broken by applying the differing conceptual perspectives identified in during the language analysis in Section 4.5.2 to the broad categories. This application of context can best be described by the Internet of Medical Things (IoMT) and the Healthcare Internet of Things (HIoT). Both are concerned with healthcare and IoT; however, conceptually, they can be separated. As IoMT denoted medical, it can be said to apply to ‘Clinical Medical applications of IoT’, differing from HIoT, which can be applied to a more relaxed, self-help style of healthcare, outside a clinical setting. This is an example of a potential joint *reference*, as both HIoT and IoMT devices could be present in the same situation, with the same goal, separated only by the *contextual interpretation* of the device. This ‘bleed over’ is minimised by the categorisation schema presented, but can never be completely eliminated due to the application of *context*.

4.6 Conclusions

The rapidity of IoT movement in the IoT ecosystem presents significant difficulty in locking down a usable definition that can be applied with sufficient granularity for purposes of clearly identifying IoT and its derivatives. Whilst some definitions exist, those that do, either target a specific subsection of IoT and are useless outside of that capacity; or targeted at the entirety of IoT and defining the concept. The pragmatic approach of this research is somewhere in the middle, with a need for more specifics than the conceptual level, and fewer details than the specificity of the individual device level. This difference in outlook is compounded by the previously examined disagreement on terms within the ecosystem.

To remedy this, the creation of logical categories as a secondary layer between the conceptual definition and the specific aspect definitions allows for easier logical identification of the distinct areas of IoT application – without relying on specific device level identification. This gives sufficient flexibility to analyse both networks and devices, while remaining flexible enough to capture devices that may straddle the boundaries between categories; as IoT devices are wont to do.

4.7 Issues Encountered During Case

The prevalence of terms within the broader ICT ecosystem is a known issue (Thilmany, 2003). This creates an initial problem when attempting to isolate the existence of terms; although it is not insurmountable, it must be noted that the effect is magnified when an ecosystem is under such rapid evolution.

The need to argue how language is interpreted and how we define meaning is a radically different field of study than cybersecurity. Whilst exposure to different fields of study and points of view is necessary, the difficulty in constructing an argument of sufficient rigour in an unfamiliar field created a delay and increased level of difficulty in the continuation of the research. This difficulty was exemplified in the examination of terminology (Section 4.5.1), where an analysis and of language and the associated philosophy was required; a significantly different field, set of knowledge, assumptions and research processes in comparison to the cybersecurity focus of this thesis.

4.8 Changes to Research Views

No research views were invalidated in the case, given the pragmatic view of creating a boundary box to constrain the research scope.

4.9 LEARNING FROM CASE

When constructing the initial case structure, it was envisioned that the answers would flow from the questions in a direct manner, with clear and consistent structure. This case has challenged this assumption with the questions tightly interwoven and dependent on one another. Given such close cohesion and interdependence between individual questions, the separation, analysis, investigation, and subsequent answering of the questions posed would both be impractical and confusing to the researcher and reader.

A significant personal learning from this case is to be more flexible in the presentation of the argument and to adapt the presentation of the case. The contents should be presented in such a way that makes the point and argument clear to both researcher and reader; the format of which may not always be neatly structured reports, and instead may be an essay or other form of writing, or incorporate more images, tables, or other supplementary means of information portrayal.

Overall, this case (Case 1) has the designed amount influence on all subsequent cases – setting boundaries and terminology used to perform additional analysis. There are no changes to the research design resultant from this case.

5 CASE 2-A: CYBERSECURITY & NETWORK TECHNICAL CONTROLS

Technical specifications and guidance form the basis for the exacting and specific protections that must be put into place for effective cybersecurity. Without this technical guidance, the ability for a coherent implementation of cybersecurity protections is left to the best effort of any given implementation. This best-effort basis can be highly variable and is dependent on contextual implementor knowledge, monetary constraints, and time available. Despite the existing body of knowledge for cybersecurity, from technical protocols specification, authentication flows, design patterns, policy guidance and general principles for long-term management and direction (Section 2.5); if one of these aspects is missing or poorly implemented, then the overall effectiveness of protections for an implementation suffers. This existing body of knowledge has been matured via countless revisions and improvements by professionals. The complex interconnected nature of cybersecurity means that changes to one area of cybersecurity can have positive or negative effects in other areas of a system (Sussman, 2021).

This interconnected nature of the established body of knowledge means that IoT cybersecurity does not need to 'reinvent the wheel'. Instead, IoT cybersecurity can draw on the mature processes already in existence. Using the existing knowledge allows the focus of protection to be on tackling the unique challenges presented by the new technologies and applications of IoT, including device size, geospatial separation, real-world consequences, and new low power protocols (Shah & Yaqoob, 2016). These challenges are not the only aspects that need addressing, but they are some of the unique characteristics of the IoT ecosystem and the associated deployments.

In attempting to identify potential issues, this research analyses the existing guidance for IoT cybersecurity, comparing it against the existing body of cybersecurity knowledge. This comparison allows for the identification of the areas the existing body of knowledge that can be translated to the IoT ecosystem without alteration, those that require some additional information, those that cannot be translated without major work, and those that do not translate and require a new approach to effectively apply cybersecurity protections.

5.1 CONTEXTUAL NOTES

Case 2-A analyses the guidance from industry and interest groups specific to the area of IoT cybersecurity. The entire context of an organisation or individual publishing the documents is not included in the analysis – in the context of the intended audience of the document, however, is included.

5.1.1 Case-Specific Notes

- The analysis of language and IoT categorisation discussed (Case 1) previously is to be counted as an inclusion.
- When referring to an 'Organisation', during this case it will refer to an organisation that has produced a document about IoT cybersecurity.
- Each document is read, interpreted, and viewed from the lens of a cybersecurity professional performing an implementation of the document, providing the common denominator linking the analyses.

5.2 CASE SPECIFIC INPUTS

This Case, Case 2-A, takes the bounding box prescribed by Case 1 as its single contextual input.

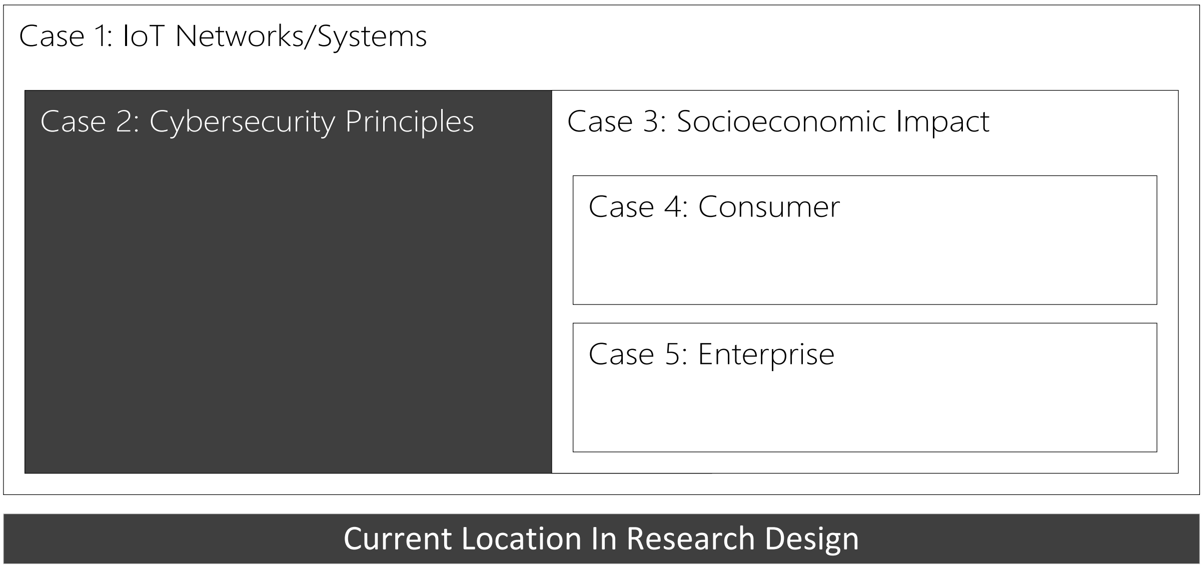
5.3 INTENDED CASE OUTPUTS

Case 2-A critically analyses the existing IoT cybersecurity guidance, with a comparison against a selected 'gold standard'. This comparison identifies the strengths, weaknesses, and omissions of the IoT cybersecurity guidance, as well as the potential easily translatable points from the existing body of knowledge.

This analysis forms the basis of a new framework for IoT cybersecurity to address the identified issues. This framework will answer the main question of this research, - "Can a framework of cybersecurity guidelines be created to improve the application and effectiveness of cybersecurity in the 'Internet of Things'?".

5.4 Case Location in the Research Design

Figure 28 denotes the current case location in the overall research design.



Case 1: IoT Networks/Systems
Case 2: Cybersecurity Principles
Case 3: Socioeconomic Impact
Case 4: Consumer
Case 5: Enterprise
Current Location In Research Design

Figure 28: Case 2-A Location in Research Design

5.5 Case Content

5.5.1 Why Current Practice Fails

The current guidance for IoT-specific cybersecurity challenges is not as mature as the existing guidance for traditional computing areas (Section 2.2)(Serral et al., 2020). Coupled with new restrictions (computing power, networking etc.) due to the nature of IoT devices, and the needs and the rapid evolution of a new ecosystem around IoT devices creates a fractured outlook for the IoT ecosystem. This lack of internal cohesion of the ecosystem creates fit for purpose deployments where each implementation is a standalone and isolated from any greater overall picture.

This fractured ecosystem means that any advice published or utilised by an organisation for their deployment is applicable in a very narrow scope and generally not applicable outside of the organisation’s specific needs. This is contrary to the existing cybersecurity knowledge base, which is platform agnostic in most cases.

5.5.2 NIST Baseline Document Overview

The National Institute of Science and Technology (NIST) publishes technical standards and conformance documents on a variety of topics, notably including cybersecurity-based documents. These documents form a core component of national, international and industry standards. The wide-ranging usage and trust in these guidance documents, coupled with extensive conformance requirements (e.g. the *Federal Information Processing Standards* (FIPS) series) and the widely cited SP 800-53 (Joint Task Force Transformation Initiative, 2013), focuses on wide-ranging technical controls and approaches to organisational cybersecurity.

The process for selecting a 'Gold Standard' for IoT cybersecurity began with a systematic search for IoT based cybersecurity guidelines. This search was initially performed using the Flinders University Library consolidated academic database search engine, and Google Scholar. This search was later expanded to include grey literature. Other documents referenced in the primary documents were also located and analysed for potential inclusion, with the goal to include the widest possible sampling of differing viewpoints regarding the application of IoT and IoT cybersecurity.

Initially, industry specific IoT guidance was located, specifically the GSMA CLP.12 Series of documents. Government produced guidance was located next, for example the ENISA *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures* (*Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures*, 2017). Extensive examination of externally referenced documents within the ENISA document was performed. Industry specific organisations and additional IoT terminology were identified from this cross-referencing activity. Further, common documents were beginning to emerge – notably, the NIST document entitled "IoT Cybersecurity Core Baseline" (Fagan et al., 2020), and other NIST documents such as FIPS, and the SP-800 series. The common reference to NIST was thematic across the IoT ecosystem, with government, industry bodies and private organisations all referring to NIST documents.

Not all documents found were selected for inclusion. The inclusion criteria were that the documents are freely available, industry acknowledged and actively supported. During this discovery phase it was discovered that many documents were either in development, marketing based, a meta-discussion or misleadingly titled, and hence these were discarded from detailed analysis.

In selecting an industry benchmark document on which to base the analysis NIST documents fit all requirements. They are publicly available, activity supported, extensively acknowledged by industry (via support, sponsorship, or document acknowledgement in publication), and have a proven history of industry adoption. For example, traditional cybersecurity protections have several documents that are identified by industry as a trusted industry benchmark, of which one is the "Framework for Improving Critical Infrastructure Cybersecurity" (National Institute of Standards and Technology, 2018).

After discovering the IoTAA, IoTA, ENISA, GSMA, Broadband Internet Technical Advisory Group (BITAG) and Council to Secure the Digital Economy (CSDE) documents, most of which referenced the NIST document "IoT Cybersecurity Core Baseline" (Fagan et al., 2020), it was determined that this NIST document should be the 'gold standard' for this research analysis.

The combination of document searching, and analysis resulted in the selection of a total of seventeen documents: one Trusted Industry Benchmark, one IoT 'Gold Standard' and fifteen IoT guidance documents. The documents selected provided a variation in publishers, target audiences, technical detail, and industry perspectives.

The NIST IoT document was developed by NIST by "…researching common cybersecurity risk managed approaches…validated using public-private process to incorporate all viewpoints" (Fagan et al., 2020), and is targeted at all aspects of the IoT ecosystem – manufacturing, integration, and consumption. The NIST IoT document is focussed on six core capabilities. These capabilities are high-level aspects of IoT cybersecurity (referred to as Cyber-Physical Systems in the document) that the IoT device should provide through some technical means, either by hardware or software. The high-level aspects are described as a "…set of device capabilities generally needed to support commonly used cybersecurity controls that protect devices as well as device data, systems, and ecosystems" (Fagan et al., 2020) and is targeted at all organisations to give a possible secure starting point for IoT ecosystems. As this is a risk-based document, the onus is on the organisation to perform a risk assessment and implement each capability in some fashion – be that in full, part, or not at all. The capabilities are discussed in detail in section 5.4.7.

5.5.3 Overview of Selected IoT Cybersecurity Documents

Each of the documents in the analysis presents its own goals and approach. To aid in identifying expectations and contextual cues relevant to each document and the research, each document is introduced to identify the overall goal and the target audience.

This thesis cross-references fifteen individual documents. These documents run the gamut from technical specifications to risk-based general practise guidelines. Specifically, they are:

- Agelight (AGELIGHT), (*AGELIGHT IoT Safety Architecture & Risk Toolkit (IoTSA) v3.1*, 2020)
- Broadband Internet Technical Advisory Group (BITAG), *(Internet of Things (IoT) Security and Privacy Recommendations*, 2016b).
- Cloud Security Alliance (CSA) IoT Working Group, *Identity and Access Management for the Internet of Things* (*Identity and Access Management for the Internet of Things - Summary Guidance*, 2016)
- Council to Secure the Digital Economy (CSDE) Convene the Conveners (C2), *(The C2 Consensus on IoT Device Security Baseline Capabilities*, 2019)
- Cellular Telecommunications Industry Association (CTIA), "CTIA Cybersecurity Certification Test Plan for IoT Devices, Version 1.0.1" (CTIA, 2018)
- European Union Agency for Network and Information Security (ENISA), (European Union & Agency for Network and Information Security, 2017)
- The European Telecommunications Standards Institute (ETSI), Baseline security recommendations for IoT in the context of critical information infrastructures. (ETSI, 2017)
- Global System for Mobile Communications Association (GSMA), Official Document CLP.11 – IoT Security Guidelines Overview Document Version 2.0
- International Electrotechnical Commission (IEC), IEC 62443-4-2, Edition 1.0, Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components (*IEC 62443-4-2*, 2019)
- Industrial Internet Consortium (IIC), Industrial Internet of Things Volume G4: Security Framework (Schrecker et al., 2016)
- The IoT Security Foundation (IoTSF), IoT Security Compliance Framework *(IoT Security Compliance Framework*, 2016)
- National Electrical Manufacturers Association (NEMA), Cyber Hygiene Best Practises, (NEMA, 2018)
- Open Connectivity Foundation (OCF), Security Specification (*OCF Security Specification Version 2.1.2, 2020)*
- Online Trust Alliance (OTA), (*IoT Security & Privacy Trust Framework v2.5*, 2017)
- Platform Security Architecture (PSA), PSA Security Model (ARM Limited et al., 2020)

5.5.4 Target Audiences

During the analysis, four discreet target audiences (of the analysed documents) were identified. Given the nature of language and the disjointed IoT ecosystem, the characteristics of the documents within target audiences are detailed below. This ensures that clear delineations are made between groups and lessen the ambiguity and confusion that comes from cross-discipline differences.

5.5.4.1 *Manufacturers / Engineers*

Documents targeted at manufacturers or engineering professionals had the following characteristics:

- Highly technical
- Specific and unambiguous
- Few (or no) generalised principles-based arguments

5.5.4.2 *Industry / Government*

Documents targeted at industry groups or government agencies had the following characteristics:

- Broad and principles-based arguments
- Aligned to a specific interest

5.5.4.3 *Governance*

Documents targeted at governance the following characteristics:

- Same broad principles-based approach as Industry / Government
- Emphasis on process and policies

5.5.4.4 *Industry*

Documents that targeted industry sectors had the following characteristics:

- Varying detail levels
- Written for an Industry Product or view of IoT
- Fit for a specific purpose
- Tightly coupled to existing infrastructure or technologies

The industry audience is distinct from the industry/government audience due to the noticeable specific commercialisation of the document or certification associated with the document. They detail an approach for an industry and are not fit for a purpose outside of that industrial sector.

5.5.5 Document Goals

Following the analysis and identification of the documents' stated targets and goals, a matrix of document to capability mapping was constructed in Figure 29: Overview of IoT Standard Capabilities. The following analysis demonstrates the grouping of target audience for each document – allowing for rudimentary management of expectations and expected level of detail.

5.5.5.1 *AGELIGHT*

Target Audience: Governance

Document Stated Goal:

The AGELIGHT *IoT Safety Architecture & Risk Toolkit Updated Addressing Hazardization* was first released in 2018 to 'adopt high-value and high-impact' security measures and privacy practices. Since its inception, the document has been updated to incorporate changing regulatory advice, including regulations from California Consumer Privacy Act (CACPA), EU GDPR and the UK Code of Practice for Consumer IoT Security. Overall, this document is aimed at regulatory and risk assessment for larger organisations seeking to ascertain overall risk profiles against a set of known and high-profile regulations.

> The IoTSA provides a blueprint to realize the promise of IoT and help avoid the pitfalls," said Craig Spiezle, Managing Director of the Agelight Digital Trust Advisory Group. "Organizations that adopt the IoTSA can maximize user safety, while making security and privacy a part of their brand promise. Those that fail risk placing society and users at risk. (https://agelight.com/iotsa-release.html)

This document is written as a listing of guidelines with mixed levels of technical details.

5.5.5.2 *BITAG*

Target Audience: Governance

Document Stated Goal:

The Broadband Internet Technical Advisory Group (BITAG) is stated as "…a non-profit, multi-stakeholder organization focused on bringing together engineers and technologists in a Technical

Working Group (TWG) to develop consensus on broadband network management practices" (*Internet of Things (IoT) Security and Privacy Recommendations*, 2016b).

This document is written as a high-level grouping of guidelines that are to be considered 'best practice'.

5.5.5.3 *CSA*

Target Audience: Governance

Document Stated Goal:

The CSA: Cloud Security Alliance (CSA) IoT Working Group, "Identity and Access Management for the Internet of Things" (*Identity and Access Management for the Internet of Things - Summary Guidance*, 2016) present a blend of security and functional requirements as their notes on secure software systems. They specify that:

> ...A reset button or functionality should automatically restore the highest level of security. The End Users of IoT devices might not be familiar with minimum security awareness aspects and might not even expect threats associated with new functionality. (*Identity and Access Management for the Internet of Things - Summary Guidance*, 2016)

This highlights the gap in knowledge of users as compared to professionals in the cybersecurity industry and provides two distinct aspects of secure software deployment – the ability to reset a device to a known good configuration and the approach of secure by default software settings when performing a reset.

This document is written as a high-level grouping of guidelines that are to be considered 'best practice'.

5.5.5.4 *CSDE*

Target Audience: Industry / Government

Document Stated Goal:

The Council to Secure the Digital Economy (CSDE) is comprised of The Consumer Technology Alliance (CTA), Association of Home Appliance Manufacturers, CableLabs and other global ICT companies to 'convene the conveners' (C2). This document is the result of this C2 group working to create the broadest and technically deep industry-based consensus on IoT security in the world. This is based on the premise that the best way to achieve security for IoT is to let the security experts develop and advance the security specifications that the market can then adopt. It also aims to provide clear and expert guidance to industry and government around IoT and casts suspicion as to the efficacy of a non-global approach to IoT security.

This document is written as a listing of guidelines with mixed levels of technical details.

5.5.5.5 *CTIA*

Target Audience: Industry / Government

Document Stated Goal:

The Cybersecurity Certification Test Plan for IoT Devices (CTIA) is a technical specification detailing the required cybersecurity measures that must be implemented to achieve certification against their IoT Cybersecurity requirements. These guidelines are designed as such that they are repeatable, verifiable, and detailed on a step-by-step basis to ensure that certification is fair. There are also restrictions based on the scope of this testing. It is assumed that Long-Term Evolution (LTE) or Wi-Fi communication is used, as other communication types are out of scope for this document, and the device would not be valid for certification. This document also prescribes a minimum level of encryption – Advanced Encryption Standard (AES) of at least 128-bit strength must be supported, along with other security-related baselines – using the standardised Syslog format for logging and ensuring that transport encryption is used.

The Cellular Telecommunications and Internet Association was renamed CTIA- The Wireless Association in 2004. The CTIA is a trade association focused on representing the wireless vendors and industry in the United States of America. As stated, the standard forms part of the formal certification suite described as:

> CTIA manages a cybersecurity certification program for Internet of Things (IoT) devices, establishing an industry baseline for device security on wireless networks. The CTIA IoT Cybersecurity Certification Test Plan supports a variety of use cases and levels of device sophistication. (CTIA, 2018).

This document is written as a list of detailed technical requirements.

5.5.5.6 *ENISA*

Target Audience: Industry / Government

Document Stated Goal:

The European Union Agency for Network and Information Security (ENISA) defines IoT as "a cyber-physical ecosystem of interconnected sensors and actuators, which enable decision making". The stated target audience includes managerial positions such as Chief Information Security Officers (CISOs) and Critical Information Infrastructure Protection Officers (CIIP), with the focus of the provided guidance on resilience, communications, interoperability – with special consideration given to privacy concerns of smart infrastructure and services.

This document is written as a high-level overview of the IoT ecosystem with a focus on cybersecurity, with example cybersecurity breaches included.

5.5.5.7 *ETSI*

Target Audience: Industry / Government

Document Stated Goal:

The European Telecommunications Standards Institute (ETSI) is a not-for-profit and independent standardisation agency focused on fulfilling European and Worldwide needs. Given the target audience of (potentially international) standards, the language here is descriptive, and the document prescribes an outcome-based approach, leaving implementation up to the manufacturer. ETSI identified that this document is not able to solve every IoT Cybersecurity issue and instead, it is focussed on the '…most significant and widespread security shortcomings' by addressing the 'technical controls and organisational policies'. These policies include newer regulatory requirements, like the GDPR. It also has some European Union specific framework creation potential.

This document is written as a list of detailed technical requirements.

5.5.5.8 *GSMA*

Target Audience: Industry

Document Stated Goal:

The Global System for Mobile Communications Association (GSMA) standards is a framework explicitly targeted at mobile networks and their associated operations. Given the breadth of mobile devices that can be connected via these specified systems and the complicated nature of the latest generation of 5G networks (Alnoman & Anpalagan, 2017), this standard focuses on secure management IoT devices and integration into the existing tooling and processes. As such, there is extensive reference to industry-specific terms such as 'Trusted Computing Base', which, while possessing a non-mobile device functional equivalent, is not an exact functional match, nor is terminology guaranteed to be applicable outside of the specific industry area.

This document is written as a high-level overview of the IoT ecosystem with a focus on cybersecurity, specific to the GSMA requirements.

5.5.5.9 *IEC*

Target Audience: Industry

Document Stated Goal:

IEC 62443-4-2, Edition 1.0, Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components (IEC 62443-4-2, 2019) presents the technical requirement and foundational requirements to meet the specifications as provided in IEC TS-62443-1-1 (International Electrotechnical Commission, 2009). This International Standard is a series of documents titled "*Industrial communication networks - IT security for networks and systems*".

This document is written as a list of detailed technical requirements.

5.5.5.10 *IIC*

Target Audience: Industry

Document Stated Goal:

The Industrial Internet Consortium (IIC) has its own detailed *Security Framework* document. It mainly focuses on providing a platform that can improve organisational level approaches and processes for Industrial IoT deployments to create a trustworthy system. This document forms part of the existing IIC testbeds and is in active usage. Given the target audience of this document, the guidance is risk-based, aligning closely with the established practice of mitigation, avoidance, acceptance, and transference.

This document defines 'End-Point' in the IIC (Schrecker et al., 2016) as "*Endpoints* are any element of an IIoT system that has both computation and communications capabilities and exposes functional capabilities". This is broad and covers every point of communication from GSM/LTE mobile to serial-connected SCADA systems.

This document is written as both a high-level overview of the IoT ecosystem with a focus on cybersecurity and detailed technical requirements, specific to the Industrial Internet Consortium view of IoT.

5.5.5.11 *IoTSF*

Target Audience: Industry

Document Stated Goal:

The IoT Security Foundation (IoTSF), established to address cybersecurity in IoT states it mission as:

> ...to help secure the Internet of Things, in order to aid its adoption and maximise its benefits. To do this IoTSF will promote knowledge and clear best practice in appropriate security to those who specify, make and use IoT products and systems. (IoT Security Compliance Framework, 2016, pg 5).

This document is based on answering set questions to ascertain what needs to be implemented to create a secure IoT environment. The guidance is focussed on obtaining devices that are fit for security purposes instead of attempting to secure devices that may not provide all the requisite functionality.

This document is written as a list of detailed technical requirements.

5.5.5.12 *OTA*

Target Audience: Governance

Document Stated Goal:

The *IoT Trust Framework®* (*IoT Security & Privacy Trust Framework v2.5*, 2017) focuses on strategic level principles to secure IoT devices and their associated data through an IoT device's lifecycle, from shipping to decommission. Given its strategic outlook, this document is aimed at risk management of the entire IoT device ecosystem, not just the device itself.

This document is written as a high-level grouping of guidelines that are to be considered 'best practice'.

5.5.5.13 *NEMA*

Target Audience: Manufacturers / Engineers

Document Stated Goal:

The National Electrical Manufacturers Association "Cyber Hygiene Best Practices" outlines its document as "*…identifies a set of industry best practices and guidelines that electrical equipment and medical imaging manufacturers can implement to raise their level of cybersecurity sophistication in their manufacturing facility and engineering processes*" (NEMA, 2018). This document is based on the common layouts and deployments that NEMA view as important, the key principles of cybersecurity and how to apply them to the depicted network layouts.

This document is written contains both a high-level overview of the IoT ecosystem with a focus on cybersecurity and detailed technical requirements, specific to the NEMA view of IoT.

5.5.5.14 *OCF*

Target Audience: Manufacturers / Engineers

Document Stated Goal:

The Open Connectivity Foundation (*OCF Security Specification Version 2.1.2*, 2020) document specifies the security objectives, philosophy, resources, and mechanism that impacts the rest of the OCF standard and links to ISO/IEC 30118-1:2018 (Information technology -- Open Connectivity Foundation (OCF) 399 Specification -- Part 1: Core specification). This document forms part of the OCF published standard and is written to supplement OCF's security architecture. As this document is part of a published standard, the document is specific and unambiguous to allow for certification.

This document is written as a list of detailed technical requirements.

5.5.5.15 *PSA*

Target Audience: Manufacturers / Engineers

Document Stated Goal:

Platform Security Architecture (PSA) also contains the PSA Security Model (PSA-SM) and has a stated purpose of:

> The PSA Security Model defines the foundation for establishing that trust by defining the security capabilities that CSPs [Cloud Security Providers] can rely on; Providing technical

input for the business commitment between different ecosystem entities and Establishing common technical definitions and terminology. (*Arm® Platform Security Architecture Security Model 1.0*, 2019).

Fundamentally, this document is a hardware-based specification and is similar to the OCF document – technical, precise, and unambiguous in requirements and optional features. The PSA-SM should be viewed as supplemental material to the main 'checklist' of the PSA Checklist 'JSADEN001' (ARM Limited et al., 2020), which has the similar stated goal of "*PSA defines a common hardware and software security platform, providing a generic security foundation allowing secure products and features to be deployed*".

This document is written as a list of detailed technical requirements.

5.5.5.16 *Target Audience Summary*

Table 16 depicts the mappings of documents from the NIST baseline document and their extracted target audiences.

Table 16: Document to Target Audience Mappings

Audience	Document
Manufacturing / Engineers	NEMA, OCF, PSA
Governance	AGELIGHT, BITAG, CSA, OTA
Industry / Government	CSDE, CTIA, ENISA, ETSI
Industry	GSMA, IEC, IIC, IoTSF

5.5.6 Document to Capability Mapping

The capabilities presented in the NIST document have been renamed by capability for clarity of purpose during analysis and to reflect the requirements of the capability more accurately. This renaming was notably required in cases where the capability covered multiple distinct areas of cybersecurity under a single heading. An example of a single capability covering multiple areas is the capability of 'Data Protection', which concerns itself with both 'Secure Data Storage' and 'Secure Data Transmission'. There is some common ground between 'Data Storage' and 'Data Transmission', but not enough commonality to treat them identically. Table 17 demonstrates the original NIST capability title mapped to the name used during analysis.

Table 17: NIST Capability to Research Capability Mapping

NIST Capability Name	Re-Named Capability
Device Identification	Logical / Physical Identifiers
Configuration	Secure Software Configuration
Data Protection	Secure Data Storage / Transmission
Logical Access to Interfaces	Secure Interface Management
Software Update	Secure Update Mechanism
Cybersecurity State Awareness	Cybersecurity State Awareness

By analysing the documents and their associated capabilities, the matrix of Figure 29: Overview of IoT Standard Capabilities was created to capture the capabilities of each document. This matrix also illustrates that each document does not always cover all capabilities provided, and there are gaps in the overall guidance available.

		IoT Guidance Documents														
	NIST Capabilities	AGELIGHT	BITAG	CSA	CSDE	CTIA	ENISA	ETSI	GSMA	IEC	IIC	IoTSF	OTA	NEMA	OCF	PSA
1	Logical / Physical Identifiers	○	○	●	●	●	○	○	●	○	●	●	○	○	●	●
2	Secure Software Configuration	○	●	●	○	○	●	○	○	●	○	●	●	○	●	●
3	Secure Data Storage / Transmission	●	●	○	●	●	●	●	●	●	●	●	●	○	●	●
4	Secure Interface Management	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
5	Secure Update Mechanism	●	●	○	●	●	●	●	●	●	●	●	●	●	●	●
6	Cybersecurity State Awareness	○	○	○	●	●	●	●	●	●	●	●	○	●	●	●

Figure 29: Overview of IoT Standard Capabilities

Given the coverage shown in Figure 29, the use of the NIST document as the baseline must be defended at this stage. Specifically, that the PSA and OCF documents appear to cover each of the mandated capabilities, so it must be examined as to why they are not used as the baseline instead of the NIST document. The answer is applicable to every single document analysed and listed in Figure 29 – each one tackles and presents their own, fit-for-purpose view of what IoT networks and the associated cybersecurity approach should be. This narrow view renders the guidance outside the intended audience somewhat useful at best and woefully inadequate at worst. As such, the higher level and broader NIST document stands as the base document, as it presents an ecosystem wide, implementation agnostic view of IoT cybersecurity.

5.5.7 Capability Explanation

Each of the six cybersecurity capabilities in the NIST document a unique impact, importance, and interrelation to the other capabilities. Each of the capabilities is discussed below to present some of the key aspects when regarding cybersecurity, and some of the potential interrelations.

5.5.7.1 *Capability 1: Logical / Physical Identifiers (NIST: Device Identification)*

Logical / Physical Identifiers are the ability to identify individual devices in a unique manner. This capability covers both logical and physical identification.

5.5.7.1.1 Importance

Using a unique identifier for hardware, and sometimes software, is a common practice in many industries not just Information Communication Technology. Motor vehicles have Vehicle Identification Numbers, consumer goods have serial numbers, and ICT networking has IP Addresses. Each of these is either a physical or logical identifier that allows for a piece of hardware or software to be identified uniquely.

When attempting to use these identifiers for cybersecurity purposes, the physical and logical identifiers tackle different areas of cybersecurity. Logical identifiers are usually for Security Information and Event Management (SIEM) or Network Monitoring tools to track a device's presence within a logical network. Physical identifiers are usually used for hardware or inventory management, allowing devices to be commissioned, decommissioned, or repaired.

This distinction between logical and physical identifiers means that each comes with its own distinct challenges when used as a part of a cybersecurity effort. Logical identifiers can be spoofed and manipulated by attackers whilst physical identifiers must consider physical access. Both fields are different types of entities, and will require different measures to apply cybersecurity soundly.

5.5.7.2 *Capability 2: Secure Software Configuration (NIST: Configuration)*

Secure Software Configuration is described as the ability for software running on a device or the associated systems to be configured. These configurations should be allowed only by authorized persons. This capability combines multiples areas of cybersecurity, including authentication, authorization, and secure software.

5.5.7.2.1 Importance

Secure software configuration enables other capabilities to be varied in strength of protection or even removed if desired by the user. Common actions include changing passwords, changing cryptographic keys or certificates, modifying services, changing communication ports or endpoints, and enabling or disabling features. This ability to configure devices to match the required security approach (which is highly contextual and unique to each implementation) enables devices to be more secure.

5.5.7.3 *Capability 3: Secure Data Storage / Transmission (NIST: Data Protection)*

Secure Data Storage / Transmission is the ability of a device to protect both the data it stores and the data it transmits via encryption. The intent is to prevent unauthorized access or modification of data at all stages of its lifecycle, from creation to deletion.

5.5.7.3.1 Importance

Secure data storage is arguably the most crucial part of modern ICT systems – protecting the data generated and used in operations. This capability assists in data protection using cryptographic controls at all stages of its lifetime (creation, transmission, and storage), and allows for the secure enforcement of access management when coupled with authentication and authorization. This protection allows for the enhancement of the confidentiality and integrity of data via cryptography. Some everyday actions include hardware-backed cryptographic storage, remote secure data destruction, and user-configurable security levels.

5.5.7.4 *Capability 4: Secure Interface Management (NIST: Logical Access to Interfaces)*

Secure Interface Management is the ability for a device to restrict access to both physical and logical interfaces. This includes the protocols and services running on those interfaces.

5.5.7.4.1 Importance

Access restriction relies on a fundamental pillar of all cybersecurity actions - authentication. Without knowing that an actor is who they purport themselves to be, no additional protections can be built. Authorization cannot be used to restrict actions and non-repudiation becomes flawed. This ties directly to secure interface management, as without authentication and authorisation, it is effectively impossible to perform secure interface management. This management is applied to follow another facet of cybersecurity – the principles of least access and privilege. Generally, these actions include requires authentication, and applying authorisation to permitted actions against a given endpoint.

5.5.7.5 *Capability 5: Secure Update Mechanism (NIST: Software Update)*

A secure update mechanism is described as the ability for a device to have its software updated by authorized entities, using a secure and configurable mechanism. This capability depends on the ability to configure the software and the ability to transmit and protect the update files securely.

5.5.7.5.1 Importance

The increase in complexity of devices and deployments has created an ecosystem that enables attacks of differing magnitude from multiple possible vectors. To prevent attacks like update poisoning, which allows for a single exploit to be magnified exponentially should the malicious payload be pushed to devices, this capability requires multiple aspects of cybersecurity - authentication, authorization, non-repudiation, and cryptographic techniques. In terms of other capabilities, it is similarly expansive, requiring all other capabilities in some fashion.

5.5.7.6 *Capability 6: Cybersecurity State Awareness (NIST: Cybersecurity State Awareness)*

Cybersecurity State Awareness is the ability for a device to report its own security state, it may also be described as security monitoring. This capability depends on all previous capabilities (1-5) to correctly function.

5.5.7.6.1 Importance

The need for a device to be cognizant of its own operating parameters and make decisions based on a known state (to raise an alert when necessary) depends on all aspects of the previously mentioned capabilities (capabilities 1-5) to perform this task. This expansion of simple reporting to dynamic action and response is associated with the new security product and method generation.

5.5.8 Document Overview: AGELIGHT

The current document under analysis against the gold standard is AGELIGHT. (AGELIGHT IoT Safety Architecture & Risk Toolkit (IoTSA) v3.1, 2020).

5.5.8.1 *Capability to Section Mapping*

Table 18 details the sections of the reviewed document (AGELIGHT) as they relate to the NIST Security Capabilities described in the "*IoT Device Cybersecurity Capability Core Baseline*". This document (AGELIGHT) is not prescribed in all capabilities, denoted by a '-'.

Table 18: AGELIGHT to NIST Document Mappings

Benchmark Capability (NIST)	Section (AGELIGHT)
Logical / Physical Identifiers	-
Secure Software Configuration	-
Secure Data Storage & Transmission	5, 7, 18, 24, 25, 34
Secure Interface Management	10, 13, 14, 15
Secure Update Mechanism	1, 2 ,4
Cybersecurity State Awareness	-

5.5.8.2 *Common Sections*

AGELIGHT has no document sections that are mentioned in more than one capability.

5.5.8.3 *Capability Analysis*

The following section compares the guidance in the current document to the selected 'Gold Standard'.

5.5.8.3.1 Capability: Logical / Physical Identifiers

This section is not cross-referenced in the NIST Document.

5.5.8.3.2 Secure Software Configuration

This section is not cross-referenced in the NIST Document.

5.5.8.3.3 Secure Data Storage & Transmission

5.5.8.3.3.1 Strengths

The practice of salting (adding additional random characters to a password) and hashing user credentials is an accepted approach to minimising the risk of stolen credentials. If both are done, the need for specific guidance decreases, but the strength of protections can be enhanced by guidance on acceptable hashing algorithms and salt sizes.

The ability to perform a device reset depends on the Secure Software Configuration capability to be performed correctly. Device reset covers purging the device of data and specifically mandates that any cloud-based backups or recovery data must also be removed. This ability is specific to personal data – not site generic settings like where devices are located or customized profiles for a site or home. It also combines the ability to export data. The ability to restore a device from that backup is only implied.

Differing from a device reset, the ability to factory reset a device is a potential precursor to transferring a device. The key differentiating factor is that the factory reset will purge all data, including device configuration and profile data, resetting it to a clean or as-new slate.

5.5.8.3.3.2 Weakness

The presented argument that *"...Encryption of data has become the norm and is increasingly stipulated as a baseline security requirement*" is broad and generic. Given that the prescribed approach to encryption is the utilisation of current and generally accepted cryptographic suites and associated protocols, it is possible to select a vulnerable algorithm that still fits the guidelines. There is mention of Personally Identifiable Information (PII) that may be stored on an IoT device and the different regulations that govern such data. Whilst this starts as a strength, it fails to link to acceptable guidance on strong encryption algorithms or warn against the use of depreciated or attackable algorithms. It also does not warn against the dangers of 'hand-rolling' cryptographic algorithms. Whilst it is implied that this should not be done, it is not directly mentioned as a concern.

A single reference to Bluetooth sniffing also mentions that greater physical security implications may be at play if an adversary is sniffing the comparatively short-range (compared to Wi-Fi) Bluetooth based traffic. The mention of this is not an inherent weakness, however, the lack of expansion and the brief mention in the document downgrade it to a weakness, as it conflates physical security measures with a Bluetooth protocol security measure.

5.5.8.3.3.3 Other Observations

The guidance for Bluetooth is only a *recommendation*. It recommends that all Bluetooth connections should be encrypted when transmitting *"... User ID's passwords and other sensitive information"*. This is potentially a strength but is not mandated, reducing its usefulness – it also leaves sensitive information up to the implementation, which can lead to a weakness.

There are internal document references that have greater and unexplained implications. For example, the reference between Bluetooth communication and cryptography implies that credentials should be salted, hashed, and encrypted by the acceptable suite of cryptographic functions. The acceptable encryption algorithm or preferred methods are not directly listed.

There is also specific mention of data retention and collection policies. Whilst this can be a regulatory and compliance move, it is not directly applicable to the cybersecurity of IoT. It guides cybersecurity implementation, but it is not a directly implementable control. It is best described as an influencing factor in cybersecurity controls – mainly data storage and management. This policy itself will be influenced by external forces like the European Union's GDPR and similar legislation.

5.5.8.3.3.4 Capability Summary

Table 19 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 19: AGELIGHT Secure Data Storage & Transmission Summary

Strengths	Weaknesses	Other Observations
Use Encryption	Lack of guidance on what constitutes good encryption Fails to mention not to use depreciated / weak algorithms Does not warn against hand-rolling cryptography	-
Salt & Hash User Credentials	Lack of guidance on acceptable hash algorithms or salt-sizes	Implying that credentials should be salted, hashed, and encrypted, without explicitly stating
Have Policies	No mention of other policies, mainly regulatory concerns	Data Retention & Collection Policies should be disclosed
Device Reset	Device & Cloud Data Keep the device profile Settings	Backup / Restore function implied
Factory Reset	Complete Reset of all data	Possible Transfers of Ownership

5.5.8.3.4 Secure Interface Management

5.5.8.3.4.1 Strengths

The document prescribes a multilayer approach to the management of logical interfaces covering testing, usage scenarios, aspects of desired (device & user) behaviour, some vulnerability management, and the principles of least access. Many of these actions depend on the secure update mechanisms, secure data transmissions and secure software configuration capabilities to perform the needed operations.

The securing of all unneeded ports and connections is mandated. This includes removing debug and test modes and disabling ports and services when they are not in active use. If they must be left open and on a non-secure network, then they should be secured with specific rigorous actions.

Coupling this removal of un-needed ports with both Multi-Factor Authentication (MFA) and an out-of-band password recovery mechanism, restricting of using any type of default credentials and the addition of a client indentation and brute-force protection creates a multi-layer, best-practice based authentication mechanism.

Covering the wireless aspect, disabling automatic reconnection for wireless and forcing the usage of pins during pairing operations is required.

5.5.8.3.4.2 Weakness

The action of baking security testing into a Software Development Life-Cycle (SDLC) is not a strength without additional guidance. Security practices for SDLC vary widely between the software environment and expected output and IoT will also add additional challenges to current SDLCs. Expecting that 'code hardening' occur during these security actions is not enough information to reliably inform or perform the action.

There are also design and functionality specific required - the device is to detect and update on first boot if required, which implies it has an update mechanism built into the pre-boot environment or similar functionality before the device is ready for use. This check and associated functionality is complex and not easily implemented.

The usage and creation of brute force protection and the recognition of device sign-ins can be a complicated system that may not be able to run on an IoT device, mandating implementation of a server or device management system to complete the functionality.

5.5.8.3.4.3 Other Observations

The usage of password managers when requiring no default credentials is a strong addition, given that most password managers also contain useful generators for generating strong passwords or passphrases.

5.5.8.3.4.4 Capability Summary

Table 20 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 20: AGELIGHT Secure Interface Management Summary

Strengths	Weaknesses	Other Observations
Interface Management	Not all protections are under the control of end-users	-
No Default Credentials	-	Password managers are a good mention
Remove Debug & Test Modes	-	-
Strong Pairing & Connections for Wireless Communications	-	-

5.5.8.3.5 Secure Update Mechanism

5.5.8.3.5.1 Strengths

Disclosing the security and update patches during a device lifecycle, whilst a modern and expected practice is not always implemented or adhered to. Mandating that patches, especially for security, are provided and are actively developed throughout the product's lifecycle. This ability is enhanced by the mandate of an automated update mechanism that includes cryptographic signing and verification of the update payload.

User Experience (UX) enhancement is the ability to differentiate and warn users if the updates are automated or manual. This ability to inform users, allows users to defer the updates that are not wanted or may have been released an inopportune time.

5.5.8.3.5.2 Weakness

Implementing deferrable, notifiable updates is a complicated and resource-intensive task that may not be implemented correctly or fully on IoT devices. Anything beyond the most basic of these functions usually requires support from a server-based implementation to support the devices and perform the scheduling or computationally expensive operations.

5.5.8.3.5.3 Other Observations

There is nothing mentioned of mobile device management, and the need to manage dozens on dozens of devices and their individual profiles and associated update or patch status is a complicated task.

5.5.8.3.5.4 *Capability Summary*

Table 21 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 21: AGELIGHT Secure Update Mechanism Summary

Strengths	Weaknesses	Other Observations
Security Patches	Notifications, Deferrable updates and 'UX' focussed options may not be standalone on an IoT device	-
-	-	Mobile Device management is already a challenge (Yamin & Katt, 2019)

5.5.8.3.6 Cybersecurity State Awareness

This section is not cross-referenced in the NIST Document.

5.5.8.3.7 Overall Summary Table: AGELIGHT

Table 22 is a summary of all identified strengths, weaknesses and other notes gathered from the AGELIGHT document.

Table 22: AGELIGHT Overall Summary

Benchmark Capability (NIST)	Strengths	Weaknesses	Other Observations
Secure Data Storage & Transmission	Use Encryption	Lack of guidance on what constitutes good encryption Fails to mention not to use depreciated / weak algorithms Does not warn against hand-rolling cryptography	-
	Salt & Hash User Credentials	Lack of guidance on acceptable hash algorithms or salt-sizes	Links to internal document section, implying that credentials should be salted, hashed, and/or encrypted – this is not explicitly stated

	Have Policies	No mention of other policies, mainly regulatory concerns.	Data Retention & Collection Policies should be disclosed
	Device Reset	Device & Cloud Data Keep the ‘Device Profile’ Settings	Backup / Restore function implied
	Factory Reset	Complete Reset of all data	Possible Transfers of Ownership
Secure Interface Management	Interface Management	Not all protections are under control of end users	-
	No Default Credentials	-	Password managers is a good mention
	Remove Debug & Test Modes	-	-
	Strong Pairing & Connections for Wireless Communications	-	-
Secure Update Mechanism	Security Patches	Notifications, Deferrable updates and UX focussed options may not be standalone on an IoT device	-
	-	-	Mobile Device management is already difficult, and (usually) requires 3rd party tooling.

5.5.9 Document Overview: BITAG

The current document under analysis against the gold standard is Broadband Internet Technical Advisory Group (BITAG) (Internet of Things (IoT) Security and Privacy Recommendations, 2016b).

5.5.9.1 *Capability to Section Mapping*

Table 23 details the sections of each reviewed document as they relate to the NIST ‘Security Capabilities’ described in the “*IoT Device Cybersecurity Capability Core Baseline*”. This document (BITAG) is not prescribed in all capabilities, denoted by a ‘-‘.

Table 23: BITAG to NIST Document Mappings

Benchmark Capability (NIST)	Section (BITAG)
Logical / Physical Identifiers	-
Secure Software Configuration	7.1
Secure Data Storage & Transmission	7.2, 7.10

Secure Interface Management	7.1, 7.2, 7.3, 7.6
Secure Update Mechanism	7.1
Cybersecurity State Awareness	-

5.5.9.2 *Common Sections*

The following sections in the BITAG document appear under multiple capabilities.

- BITAG Section 7.1: IoT Devices Should Use Best Current Software Practices
- BITAG Section 7.2: IoT Devices Should Follow Security & Cryptography Best Practices

5.5.9.2.1 BITAG: 7.1 IoT Devices Should Use Best Current Software Practices

5.5.9.2.1.1 Strengths

The usage of an update mechanism that is both secure and automated, explicitly acknowledging that new vulnerabilities will be found over time. There is additional data provided within this capability that is not directly relevant and detracts from the key information for secure update mechanisms.

The guidance is about the usage of strong authentication by default. This is realised by not using easily guessed username and password combinations; coupled with manufacturer processes, such as shipping devices with fixed passwords that require change as part of a setup or shipping devices with a unique password that is physical affixed to the device. The inclusion of remote access to these same requirements prevents oversight of not including remote access mechanisms from using strong authentication.

The suggestion that device will actively prevent itself from being configured in such a way as to decrease the security is a possible aspect; however, a warning may be more prudent, as security is not the be-all-end-all of device operation, and there are always exceptions to any defaults that may be set by a manufacturer.

5.5.9.2.1.2 Weaknesses

The update system presented mentions multiple differing approaches, and the claims much without substantial explanation. The update mechanism described is on that should be automatic, invisible to users and opt-out in terms of functionality and configuration, presenting a potentially severe issue. This section is claimed to be based on human-computer interaction studies, but no studies are referenced to give credence to this claim. Given the nature of IoT and the general need for it to work with minimal human interaction, the prescribed approach may work for a subset of users. The more standardised approach is the second one that is described – the ability to configure the way the update mechanism behaves, as an IoT device in a critical role is almost certainly subject to scheduling of acceptable downtime for updates and maintenance.

5.5.9.2.1.3 Other Observations

The mandate that software ship with reasonably current software can be omitted without decreasing the effectiveness of the points made - which is that devices should have a way to update that is secure and automatable, and that due effort should be made not to ship known faulty or vulnerable software.

5.5.9.2.1.4 Section Overview

Table 24 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 24: BITAG Common Section 7.1 Summary

Strengths	Weaknesses	Other Observations
Update Mechanisms	Some approaches presented will cause unwanted behaviour of devices	Claims made without references to studies to confirm large claims Configuration is read as optional – end-user left without an operational choice
Strong Defaults	-	-
Device Testing & Hardening	-	No standards linked to further this
-	-	Reasonable current software could be omitted without detraction

5.5.9.2.2 BITAG: 7.2: IoT Devices Should Follow Security & Cryptography Best Practices

5.5.9.2.2.1 Strengths

The encryption methods presented are both nuanced to IoT devices and presented with appropriate references to substantiate the claims. The specific mention of lightweight cryptography as a possibility for lightweight devices where security is needed is a significant strength, as IoT devices are more likely to be resource-constrained than other types of devices.

The overall strength is expanded further with consideration for devices that support cloud-based operations to use the latest version of TLS and the Public Key Infrastructure (PKI) certificate-based authentication and acknowledges the issue of certificate revocation. Some specific types of communication that should be encrypted are listed, including the configuration, command and control traffic and controller to IoT device communications.

The focus is on the usage of encryption, and as such, it also follows the storage of data, not just transmission. The recommendation is to utilise secure storage for sensitive secrets such as private keys or cryptographic certificates. It is later mandated that these credentials be updated and should be unique and non-shared, particularly with certificates and public/private key pairs. This approach will introduce significant overhead and require some form of tooling to manage at scale.

Managing software dependencies is a key aspect of secure software, as self-written code for specific functions, especially cryptographic ones, is a known vector to insecure cryptographic implementations. As such, using libraries that are actively maintained helps negate this risk.

A cursory mention is made of disabling administrative functions and ports services to aid in hardening a device and reducing its attack footprint.

5.5.9.2.2.2 Weaknesses

No weaknesses were identified during comparison to the gold standard document.

5.5.9.2.2.3 Other Observations

Credentials do not always take the form of certificates of public/private key pairs – username and password combinations are more ubiquitous.

5.5.9.2.2.4 Shared Section Overview

Table 25 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis for the shared sections of the BITAG document.

Table 25: BITAG Common Section 7.2 Summary

Strengths	Weaknesses	Other Observations
Encryption	-	Credentials are not always cryptographic
Updates	Approach is not without detrimental aspects to UX	-

	Lack of references to back up claims	
Strong Defaults	-	-
-	Reasonably current software claim can be omitted without detriment to the document	-

5.5.9.3 *Capability Analysis*

The following section compares the guidance in the current document to the selected 'Gold Standard'.

5.5.9.3.1 Logical / Physical Identifiers

This section is not cross-referenced in the NIST Document.

5.5.9.3.2 Secure Software Configuration

See BITAG: 7.1 IoT Devices Should Use Best Current Software Practices.

5.5.9.3.3 Secure Data Storage & Transmission

See BITAG: 7.2: IoT Devices Should Follow Security & Cryptography Best Practices in addition.

5.5.9.3.3.1 Strengths

The management of the IoT supply chain is a complicated task requiring communication between multiple parties along the chain. Whilst a complex area, the presented aspects are detailed, including device and manufacturer-provided guidance. This guidance includes privacy policies, reset mechanisms, bug and vulnerability reporting systems, secure software supply chains, device lifecycle, and support periods with their associated patching cycles, and support contact procedures.

5.5.9.3.3.2 Weaknesses

The document directly states that "*…it is often difficult to define the roles that each party plays over time.*" (BITAG, p. 23), when concerned with the IoT device chain. When presenting an argument that the supply chain should take steps, the conjoining of devices and manufacturers, with the omission of service providers, conflates differing areas. This leaves some (manufacturer) level advice without a clear line of culpability. The most egregious of this is 'Secure Software Supply Chain' that simply states that "*…vendors and manufacturers should take appropriate measures to secure their software supply chain.*" (BITAG, Pg. 23).

5.5.9.3.3.3 *Other Observations*

No other observations were made during comparison to the gold standard document.

5.5.9.3.3.4 *Capability Summary*

Table 26 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 26: BITAG Secure Data Storage & Transmission Summary

Strengths	Weaknesses	Other Observations
Supply Chain Management	Responsibility Delegation	-
-	Service Providers are Omitted	-

5.5.9.3.4 Secure Interface Management

See BITAG: 7.1 IoT Devices Should Use Best Current Software Practices and BITAG: 7.2: IoT Devices Should Follow Security & Cryptography Best Practices in addition.

5.5.9.3.4.1 *Strengths*

The utilisation of trusted endpoints is a multifaceted issue. To have a trusted endpoint, the network must support a myriad of security technologies and the IoT devices themselves must also support a set of common functionalities to allow for the negotiation of a secure connection to a known endpoint. Given the disparate and fractured nature of the IoT ecosystem, this is difficult, and the difficulty is compounded when considering that an IoT may have multiple endpoints on a single device. A start is made via the restriction of inbound traffic to IoT devices and trust-based endpoint communication bootstrapping.

The supplemental note that devices should be able to communicate and be configured arbitrarily is desirable, and special note is made that firewalls are not a sole line of defence for an IoT device, especially for those that are utilising specialised low-power versions of protocols (E.g., 6LoWPAN) and cannot spare the overhead of processing to scan network traffic.

There is a single mention of Internet Protocol version 6 (IPv6) or Domain Name System Security Extensions (DNSSEC).

5.5.9.3.4.2 *Weaknesses*

The complicated nature of secure networking is understated by many of the prescribed actions – trusted endpoint bootstrapping may require server support or additional tooling to perform adequately for enterprise deployments and must be backed by an appropriately mature network and operations level to support the managerial overhead.

5.5.9.3.4.3 Other Observations

There are explicit recommendations that *"…to restrict the configuration of IoT device communications should not come at the cost of an open ecosystem"* (BITAG, p. 23). What precisely an open ecosystem represents is not stated.

The mention of using IP and DNS is almost required and not needed as a statement, given that almost all devices based on IoT will use IP in some fashion, particularly IPv6. The notion that simply using IP will allow for device longevity and addressing is a misleading statement.

5.5.9.3.4.4 Capability Summary

Table 27 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 27: BITAG Secure Interface Management Summary

Strengths	Weaknesses	Other Observations
Secure Endpoints	Maturity Level of Organisation Lack of detail on additional protections	"Open Ecosystem" trumps security measures
Modern Protocol Usage	-	Cursory mentions of DNSSEC/IPv6
-	-	Device Longevity is associated with DNS/IP usage

5.5.9.3.5 Secure Update Mechanism

See BITAG: 7.1 IoT Devices Should Use Best Current Software Practices.

5.5.9.3.6 Cybersecurity State Awareness

This section is not cross-referenced in the NIST document.

5.5.9.4 *Overall Summary Table: BITAG*

Table 28 is a summary of all identified strengths, weaknesses and other notes gathered from the BITAG document.

Table 28: BITAG Overall Summary

Baseline Capability	Strengths	Weaknesses	Other Observations
Secure Update Mechanism	Update Mechanisms	Some approaches presented will cause unwanted behaviour of devices	Claims made without references to studies to confirm large claims Configuration is read as optional – end-user left without an operational choice
	Updates	Approach specific is not without detrimental aspects to UX Lack of references to back up claims	-
Secure Software Configuration	Strong Defaults	-	-
	Device Testing & Hardening	-	No standards linked to further this
	-	-	Reasonable current software could be omitted without detraction
	Strong Defaults	-	-
Secure Interface Management	Secure Endpoints	Maturity Level of Organisation Lack of detail on additional protections	"Open Ecosystem" trumps security measures
Secure Data Storage & Transmission	Encryption	-	Credentials are not always cryptographic in nature
	Modern Protocol Usage	-	Cursory mentions of DNSSEC/IPv6
	-	-	Device Longevity is associated with DNS/IP usage

5.5.10 Document Overview: CSA

The current document under analysis against the gold standard is the Cloud Security Alliance (CSA) IoT Working Group, Identity and Access Management for the Internet of Things (Identity and Access Management for the Internet of Things - Summary Guidance, 2016)

5.5.10.1 *Capability to Section Mappings*

Table 29 details the sections of each reviewed document as they relate to the NIST 'Security Capabilities' described in the "IoT Device Cybersecurity Capability Core Baseline". This document (CSA) is not prescribed in all capabilities, denoted by a '-'.

Table 29: CSA Document to NIST Document Mappings

Baseline Capability (NIST)	SECTION (CSA)
Logical / Physical Identifiers	1
Secure Software Configuration	22
Secure Data Storage & Transmission	-
Secure Interface Management	2, 4, 20
Secure Update Mechanism	-
Cybersecurity State Awareness	-

5.5.10.2 *Common Sections*

The CSA document has no sections that are mentioned in more than one capability.

5.5.10.3 *Capability Analysis*

The following section compares the guidance in the current document to the selected 'Gold Standard'.

5.5.10.3.1 Logical / Physical Identifiers

5.5.10.3.1.1 Strengths

Any approach to managing IoT devices should harmonise with existing frameworks. This harmony should be done by creating a unique namespace for IoT devices, establishing a (IoT) device lifecycle, data-based security measures, local-vs-remote authorization and access, external collaboration guidelines, and the idea of a 'guest' IoT device.

5.5.10.3.1.2 Weaknesses

These presented guidelines are targeted at managerial and broad organisation level audiences, without technical information. The guidance relies on the organisation having the ability (internal or external) to perform the technical aspects securely – and handle the complexity of IoT.

5.5.10.3.1.3 Other Observations

The IAM (Identity and Access Management) style frameworks are mentioned via both acronym and its long form expansion; the IT Governance, Risk and Cyber-Risk (GRC) is mentioned only by the acronym.

5.5.10.3.1.4 Capability Summary

Table 30 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 30: CSA Logical / Physical Identifiers Summary

Strengths	Weaknesses	Other Observations
Use the existing frameworks	The managerial level approach will need technical details from other sources	Some acronyms are not explained and rely on prior knowledge

5.5.10.3.2 Secure Software Configuration

5.5.10.3.2.1 Strengths

By assuming that an end-user has no knowledge of security measures needed, changing the approach to whitelisting functions that they have explicitly approved, coupled with secure-as-possible defaults, help in allowing end-users to only enable functions that they have explicitly selected.

5.5.10.3.2.2 Weaknesses

Depending on the IoT device, secure defaults will incur development and design overhead.

5.5.10.3.2.3 Other Observations

There is no implementation guidance, and the implementation will vary widely based on the target audience and required features.

5.5.10.3.2.4 Capability Summary

Table 31 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 31: CSA Secure Software Configuration Summary

Strengths	Weaknesses	Other Observations
Secure Defaults	Developer/Design/Engineering Overhead to perform this	Wide variation based on intended destination
KISS Principle	-	-

5.5.10.3.3 Secure Data Storage / Transmission

This section is not cross-referenced in the NIST Document.

5.5.10.3.4 Secure Interface Management

5.5.10.3.4.1 Strengths

The usage of kill switch functionality can be a strength, but care must be taken to prevent misuse or non-recoverability of a device should this functionality be triggered. This kill switch is not a complete device shutdown but instead a complete severance of networking connections. This severance of networking will (if triggered) certainly interfere with other actions, such as updated and authentication, authorization and Identity and Access Management (IAM) system checks, and can potentially require physical access to restore the device, which due to the nature of IoT, may be non-trivial.

It is preferable that devices are integrated into the existing IAM systems, and that part of the deployment or provisioning process is to remove all default access accounts in favour of strong credentials. This process should also (depending on the device and requirements) enable or disable automatic updates and upgrades. This integration will depend on the specific authentication, authorisation, and security models in place within the organisation.

5.5.10.3.4.2 Weaknesses

The advice surrounding BYOD devices and consumer IoT implies the creation and adoption of a device management system. This casual mention belies the complicated nature of implementing such a system.

This document makes mention that devices should conform to standards and then mentions the Open Web Application Security Project (OWASP) as a standard. This statement is incorrect, as OWSAP is an industry set of guidance and cannot be conformance tested. This distinction is important, as anybody can claim to adhere to OWASP without doing so. This claim is contrary to standard verification procedures that adhere to international standards and follow a rigorous formal assessment and certification procedure.

5.5.10.3.4.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.10.3.4.4 *Capability Summary*

Table 32 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 32: CSA Secure Interface Management Summary

Strengths	Weaknesses	Other Observations
Remote Kill Switch	Potential Denial-of-Service	
No Defaults	-	-
Standards Conformance	Mentioned Standards are not Standards; they are Guidelines	-
Authentication & Authorization	-	Scalable, depending on the device & its situation
Use Existing IAM Systems	-	-

5.5.10.3.5 Secure Update Mechanism

This section is not cross-referenced in the NIST document.

5.5.10.3.6 Cybersecurity State Awareness

This section is not cross-referenced in the NIST document.

5.5.10.4 *Overall Summary Table: CSA*

Table 33 is a summary of all identified strengths, weaknesses and other notes gathered from the CSA document.

Table 33: CSA Overall Summary

Baseline Capabilities	Strengths	Weaknesses	Other Observations
Logical / Physical Identifiers	Use the existing frameworks	Managerial level approach, will need technical details from other sources	Some acronyms are not explained, and rely on prior knowledge
Secure Software Configuration	Secure Defaults	Developer/Design/Engineering Overhead to perform this	Wide variation based on intended destination
	KISS Principle	-	-
Secure Interface Management	Remote Kill Switch	Potential Denial-of-Service	-
	No Defaults	-	-

	Standards Conformance	Mentioned Standards are not Standards; they are Guidelines	-
	Authentication & Authorization		Scalable, depending on the device & its situation
	Use Existing IAM Systems	-	-

5.5.11 Document Overview: CSDE

The current document under analysis against the gold standard is the Council to Secure the Digital Economy (CSDE) Convene the Conveners (C2), (The C2 Consensus on IoT Device Security Baseline Capabilities, 2019).

5.5.11.1 *Capability to Section Mappings*

Table 34 details the sections of each reviewed document as they relate to the NIST 'Security Capabilities' described in the "IoT Device Cybersecurity Capability Core Baseline". This document (CSDE) is not prescribed in all capabilities, denoted by a '-'.

Table 34: CSDE Document to NIST Document Mappings

Baseline Capability (NIST)	SECTION (CSDE)
Logical / Physical Identifiers	5.1.1
Secure Software Configuration	-
Secure Data Storage & Transmission	5.1.3, 5.1.4, 5.1.5, 5.1.8, 5.1.10
Secure Interface Management	5.1.2
Secure Update Mechanism	5.1.9
Cybersecurity State Awareness	5.1.7

5.5.11.2 *Common Sections*

There are no shared sections for this document.

5.5.11.3 *Capability Analysis*

The following section compares the guidance in the current document to the selected 'Gold Standard'.

5.5.11.3.1 Logical/Physical Identifiers

5.5.11.3.1.1 Strengths

Each unique endpoint is required to have its own identifier. A list of potential aspects that may exist and require an identifier is provided, along with the potential areas that these identifiers may be used outside direct device management – such as device onboarding, authentication, authorization, access control, policy application, and device management.

The presented identifiers all come with their own caveats and applicability of range – for example, the International Mobile Equipment Identity (IMEI) or Mobile Equipment Identifier (MEID) is only useful if you have the associated networking infrastructure and capability to capture this specialised identifier.

5.5.11.3.1.2 Weaknesses

The presented controls provide a comprehensive foundation to use what is available on the device and gives an example of potential usages. The significant omissions offset this guidance as it lacks detail required to apply effective cybersecurity measures. A specific example of this is from the CSDE document *(The C2 Consensus on IoT Device Security Baseline Capabilities*, 2019) is '…storage and usage of each of the device identifier should be protected as is appropriate for that identifier' (p.11). There is no additional guidance on appropriate identifiers, selection criteria or when security measures should be in place. This lack of guidance is complicated by additional references to specialised IoT hardware functions, like 'hardware secure storage' that not all IoT devices will support. The statement that '*Provisionable identifiers should also be protected from unauthorized access, changes, and hacks.*', omits the highly variable nature of the technical controls, policy and knowledge required to implement such protections.

5.5.11.3.1.3 Other Observations

The identifiers presented are variable. Some are immutable, and others are easily spoofed or manipulated. As such, there is a reliance on external guidance for the correct situational usage of these identifiers.

5.5.11.3.1.4 Capability Overview

Table 35 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 35: CSDA Logical / Physical Identifiers Summary

Strengths	Weaknesses	Other Observations
Breadth of Identification Mechanisms	Too many identification mechanisms	Varied level of security within identifiers

-	Lack of overall detail Left to own interpretation implementation	Lack of 'Steps to Take' Guidance
Secure Hardware Storage	Assumption that devices support this	-

5.5.11.3.2 Secure Software Configuration

This section is not cross-referenced in the NIST Document.

5.5.11.3.3 Secure data Storage / Transmission

The CSDE usage of cryptography is prescribed as utilising "…open, published, proven, and peer-reviewed cryptographic methods with appropriate parameter, algorithm and option selections" (p. 16). This requirement helps prevent the 'hand-rolling' of encryption and leverages the enormous effort expended to maintain and create cryptographic protocols.

Missing are any references to other bodies that manage and define these protocols to clarify what they are or where more information can be obtained about specific algorithms or use cases.

5.5.11.3.3.1 Strengths

Data in Transit is protected – all devices should use sound and industry-tested cryptographic protocols for communication, like TLS/DTLS, IPSec, SSH or similar, with their associated standard algorithms. The distinction is made that not all data needs to be secured, so it is use-case specific. Users may elect to disable this functionality. Additional areas are listed as targets for security application, but they are not expanded on.

For example, data related to the security of the device or system, such as identity and credentials that support that identity (i.e., the configuration), should not be communicated 'in the clear'. Additionally, updates to the software and firmware should also be protected in transit.

Data at rest is protected, and this requires balance. It is not required that all data be encrypted, especially as computation power is limited for IoT devices. The phrase 'sound cryptographic means' suffers that same lack of technical guidance as all cryptographic information in this section.

5.5.11.3.3.2 Weaknesses

No weaknesses identified during comparison to the gold standard document.

5.5.11.3.3.3 Other Observations

All communication should use industry-accepted protocols. This mandates that the device is to apply widely used protocols and not use any deprecated or replaced versions of said protocols.

5.5.11.3.3.4 Capability Overview

Table 36 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 36: CSDE Secure Data Transmission & Storage Summary

Strengths	Weaknesses	Other Observations
All Data in Transit Protection	-	All data should be security transmitted – not just administrative
Use Verified Cryptography	-	'Replaced versions' of protocols is odd wording – 'newest available' is clearer
Encrypted Data at Rest	-	A notice about not needing to encrypt everything would be beneficial

5.5.11.3.4 Secure Interface Management

5.5.11.3.4.1 Strengths

Enable device-level operational and management capabilities by requiring user authentication to read or modify the software, firmware, and configuration. This authorisation should include means to ensure device-unique credentials for administrative access, and by protecting access to interfaces. This is preferably implemented via some form of One-Time Password (OTP) with Multi-Factor Authentication (MFA). OTP Passwords are required to be a decent length (equal or greater than six characters) without OTP code cross-pollution between users.

5.5.11.3.4.2 Weaknesses

Password complexity is mandated and specifies length. While there is a benefit to expanding the keyspace via complexity to prevent brute force attacks, the usage of passphrases and increasing length is now the industry preferred approach instead of arbitrary complexity requirements.

The information provided is a blend of Operations System Security configuration, default settings management, invalid configuration rejection, and device-specific operations. While representing the interconnection nature of cybersecurity, this blend of requirements causes an increase in the comprehension level required to ascertain the steps that need to be taken.

5.5.11.3.4.3 Other Observations

Devices will have varied support for the listed authentication and authorization functions.

5.5.11.3.4.4 Capability Overview

Table 37 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 37: CSDE Secure Interface Management Summary

Strengths	Weaknesses	Other Observations
OTP Passwords	Blurred responsibility capability of OTP Password Complexities Default Rejections	-
Protection of Sensitive Functions	-	Devices will have varied support

5.5.11.3.5 Secure Update Mechanism

5.5.11.3.5.1 Strengths

The ability to patch devices securely is challenging enough before the overhead of IoT complexity. Acknowledging that the ability to patch devices will vary on individual device complexity, manageability and use-cases is a good start to tailoring a patch cycle to fit the prescribed audience.

The unique application of IoT to short-term or single usage (e.g., smart shipping labels) creates additional complexity that is must be accounted for; patching such single-use devices should still be possible. Time constraints and update procedures may necessitate detection and replacement instead of remediation, given the potential numerical scale of such devices.

These patches overall should have some form of cryptographic verification – application signing and package hashing are some possible mechanisms. Ideally, these updates are delivered over-the-air (OTA) or over-the-wire (OTW).

5.5.11.3.5.2 Weaknesses

No weaknesses were identified during comparison to the gold standard document.

5.5.11.3.5.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.11.3.5.4 Capability Overview

Table 38 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 38: CSDE Secure Update Mechanism Summary

Strengths	Weaknesses	Other Observations
OTA / OTW Patching	-	-
Patch Verification	-	-

5.5.11.3.6 Cybersecurity State Awareness

5.5.11.3.6.1 Strengths

Monitoring the state of an IoT device is impossible without thorough auditing and monitoring of all aspects of the device. While a device does not need to keep an infinite number of events locally, this aspect of storage will most likely be transferred to a gateway or edge-computing device in charge of aggregating many IoT devices. Some relevant events are listed as targets for monitoring – failure to boot, failed integrity checks and excessive logins.

5.5.11.3.6.2 Weaknesses

A limited list of probable security-based events.

5.5.11.3.6.3 Other Observations

There is a reference that clear audit trails and event logs aid in digital forensics if required after an adverse event.

5.5.11.3.6.4 Capability Overview

Table 39 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 39: CSDE Cybersecurity State Awareness Summary

Strengths	Weaknesses	Other Observations
Device Specific Events	Lacklustre list of probable security-based events	-
Gateway Based Logging	-	Does require that the device support this
-	-	Reminder that not logging makes forensic analysis much more difficult

5.5.11.4 *Overall Summary Table: CSDE*

Table 40 is a summary of all identified strengths, weaknesses and other notes gathered from the CSDE document.

Table 40: CSDE Overall Summary

Benchmark Capability	Strengths	Weaknesses	Other Observations
Logical / Physical Identifiers	Breadth of Identification Mechanisms	Too many identification mechanisms	Varied level of security within identifiers
	-	Lack of overall detail Left to own interpretation implementation	Lack of 'Steps to Take' Guidance
	Secure Hardware Storage	Assumption that devices support this	
Secure Data Storage / Transmission	All Data in Transit Protection	-	All data should be security transmitted – not just administrative
	Use Verified Cryptography	-	'Replaced versions' of protocols is odd wording – 'newest available' is clearer
	Encrypted Data at Rest	-	A notice about not needing to encrypt everything would be beneficial
Secure Interface Management	OTP Passwords	Blurred responsibility capability of OTP Password Complexities Default Rejections	-
	Protection of Sensitive Functions	-	Devices will have varied support
Secure Update Mechanism	OTA / OTW Patching	-	-
	Patch Verification	-	-
	Device Specific Events	Lacklustre list of probable security-based events	

Cybersecurity State Awareness	Gateway Based Logging	-	Does require that the device support this
	-	-	Reminder that not logging makes forensic analysis much more difficult

5.5.12 Document Overview: CTIA

The current document under analysis against the gold standard is the Cellular Telecommunications Industry Association (CTIA), "CTIA Cybersecurity Certification Test Plan for IoT Devices, Version 1.0.1" (CTIA, 2018).

5.5.12.1 *Capability To Section Mappings*

Table 41 details the sections of each reviewed document as they relate to the NIST 'Security Capabilities' described in the "IoT Device Cybersecurity Capability Core Baseline". This document (CTIA) is not prescribed in all capabilities, denoted by a '-'.

Table 41: CTIA Document to NIST Document Mappings

Baseline Capability (NIST)	SECTION (CTIA)
Logical / Physical Identifiers	4.13
Secure Software Configuration	-
Secure Data Storage & Transmission	4.8, 5.14, 5.15
Secure Interface Management	3.2, 3.3, 3.4, 4.2, 4.3, 4.9, 5.2
Secure Update Mechanism	3.5, 3.6, 4.5, 4.6, 5.5
Cybersecurity State Awareness	4.7, 4.12, 5.7, 5.16

5.5.12.2 *Common Sections*

This document has no common sections.

5.5.12.3 *Capability Analysis*

The following section compares the guidance in the current document to the selected 'Gold Standard'.

5.5.12.3.1 Logical/Physical Identifiers

5.5.12.3.1.1 Strengths

This industry standard focuses on creating a testing plan that can be used to ensure a given IoT device can be identified. It does not mandate that any specific identifier is used, just that one is available, and you can make use of it for identification purposes. Additional references to NIST standards provide additional guidance and explicit criteria to confirm the function of the capability.

5.5.12.3.1.2 Weaknesses

This testing plan leverages additional frameworks, including NIST, to address the technical aspects of cybersecurity. The CTIA document itself does not hold all technical details; instead, it specifies a wealth of additional technical knowledge from external sources. The resulting minor weakness is that some of the more pertinent information could have been included as an expected starting point.

5.5.12.3.1.3 Other Observations

Generally, the information is focussed on industry interoperability, and certification and not cybersecurity certification.

5.5.12.3.1.4 Capability Overview

Table 42 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 42: CTIA Logical / Physical Identifiers Summary

Strengths	Weaknesses	Other Observations
Agnostic Testing Plan	-	Security vs. interoperability standards
External Standards	-	Some additional data could be included

5.5.12.3.2 Secure Software Configuration

This capability is not cross-referenced in the NIST document.

5.5.12.3.3 Secure Data Storage & Transmission

5.5.12.3.3.1 Strengths

The encryption requirements mandate that devices utilise modern encryption with proven protocols and sets a minimum level of encryption that is acceptable. These protocols include TLS, DTSL, SSH or IPsec. The device must also be able to create and validate Rivest-Shamir-Adleman (RSA) / Elliptic Curve Digital Signature Algorithm (ECDSA) signatures.

5.5.12.3.3.2 Weaknesses

Whilst the protocols presented are an acceptable list, it does not mention the need to utilise the latest version of these protocols, as TLS 1.0, 1.1 and 1.2 are subject to flaws and attacks that may compromise cybersecurity.

5.5.12.3.3.3 Other Observations

The device must store and retrieve data that meets the mandated encryption standard, requiring a filesystem that supports encrypted files and the appropriate technical mechanisms.

5.5.12.3.3.4 Capability Overview

Table 43 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 43: CTIA Secure Data Storage & Transmission Summary

Strengths	Weaknesses	Other Observations
Secure Protocols	Usage of Deprecated protocol versions	-
Cryptographic Functions	-	Filesystem & Networking Support required

5.5.12.3.4 Secure Interface Management

5.5.12.3.4.1 Strengths

The focus is on password and Multi-Factor Authentication (MFA), specifically One Time Passwords (OTP), coupled with the ability to managed and distribute access controls from an Enterprise Management System (EMS), allowing for role-based authentication/authorisation (RBAC).

Specifically, passwords must have unique default per device, reject defaults during operation, be alterable locally, adhere to a password complexity requirement, and not be accessible from other users. OTP's must not be accepted once used, not be accepted on a different device, not be accepted more than once, and be at least six characters in length. Finally, the EMS must not allow a device to set a forbidden password, lockout devices due to inactivity, prevent login from disabled roles, and allow devices to implement a rate-limit or blocking mechanism.

5.5.12.3.4.2 Weaknesses

The requirement that local passwords do not contain "… several repetitive or sequential characters" (CTIA, 2018. p.13) is anachronistic, as the current best practise is to use length instead of arbitrary complexity requirement.

5.5.12.3.4.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.12.3.4.4 Capability Overview

Table 44 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 44: CTIA Secure Interface Management Summary

Strengths	Weaknesses	Other Observations
Integration Verification	-	-
Device Verification	-	-
OTP/MFA & RBAC	An unclear password complexity requirement	-

5.5.12.3.5 Secure Update Mechanism

5.5.12.3.5.1 Strengths

A device must support non-destructive patching to add new features, fix software bugs, and mitigate vulnerabilities. This update requirement may be met via manual or automatic patching; however, it must include some form of verification (e.g., Digitally Signed Software) to ensure that patches can only be installed from an authorized source. When integrating with an Enterprise Management System (EMS), this patching should be schedulable.

5.5.12.3.5.2 Weaknesses

No weaknesses were identified during comparison to the gold standard document.

5.5.12.3.5.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.12.3.5.4 Capability Overview

Table 45 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 45: CTIA Secure Update Mechanism Summary

Strengths	Weaknesses	Other Observations
Digitally Signed Software	-	-
Automatic & Manual Updates	-	-

5.5.12.3.6 Cybersecurity State Awareness

5.5.12.3.6.1 Strengths

There are detailed requirements on logging, integration into an EMS, criticality-based deadlines, standard formatting, prescribed minimum event-level captures, with explicitly mentioned malicious actions of log manipulation and physical tampering as points of awareness. Specific mention of requiring adherence to the already mandated transmission security aspects.

5.5.12.3.6.2 Weaknesses

Slight lack of clarity on the different logging locations; the audit log is a local, disk-based log, and an EMS should be a remote Syslog-esq server that takes a copy of the log events.

This section of guidance is a signpost that threat monitoring should occur but is specified as "*Confirm that the device supports logging of anomalous or malicious activity based on configured policies and rules*" (CTIA, p. 24), without further expansion.

5.5.12.3.6.3 Other Observations

Syslog traffic is not transmitted securely by default and incurs an overhead of knowledge and time to secure.

5.5.12.3.6.4 Capability Overview

Table 46 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 46: CTIA Cybersecurity State Awareness Summary

Strengths	Weaknesses	Other Observations
Local & Remote Logging	Clarity on 'Local' vs. Remote Requirements	Syslog is not secure by default, with some minor

		configuration overhead
-	Threat monitoring is severely lacking in detail and could easily be removed	-

5.5.12.4 *Overall Summary Table: CTIA*

Table 47 is a summary of all identified strengths, weaknesses and other notes gathered from the CTIA document.

Table 47: CTIA Overall Summary

Baseline Capability	Strengths	Weaknesses	Other Observations
Logical / Physical Identifiers	Agnostic Testing Plan	-	Security vs. interoperability standards
	External Standards	-	Some additional data could be included
Secure Data Storage and Transmission	Secure Protocols	Usage of Deprecated protocol versions	-
	Cryptographic Functions	-	Filesystem & Networking Support required
Secure Interface Management	Integration Verification	-	-
	Device Verification	-	-
	OTP/MFA & RBAC	An unclear password complexity requirement	-
Secure Update Mechanism	Digitally Signed Software	-	-
	Automatic & Manual Updates	-	-
Cybersecurity State Awareness	Local & Remote Logging	Clarity on 'Local' vs. Remote Requirements	Syslog is not secure by default, with some minor configuration overhead
	-	Threat monitoring is severely lacking in detail and could easily be removed.	-

5.5.13 Document Overview: ENISA

The current document under analysis against the gold standard is the European Union Agency for Network and Information Security (ENISA), (European Union & Agency for Network and Information Security, 2017).

5.5.13.1 *Capability To Section Mappings*

Table 48 details the sections of each reviewed document as they relate to the NIST 'Security Capabilities' described in the "IoT Device Cybersecurity Capability Core Baseline".

Table 48: ENISA Document to NIST Document Mappings

Baseline Capability (NIST)	SECTION (ENISA)
Logical / Physical Identifiers	GP-PS-10
Secure Software Configuration	GP-TM-06
Secure Data Storage & Transmission	GP-OP-04, GP-TM-02, GP-TM-04, GP-TM-14, GP-TM-24, GP-TM-32, GP-TM-34, GP-TM-35, GP-TM- 39, GP-TM-40
Secure Interface Management	GP-TM-08, GP-TM-09, GP-TM-21, GP-TM-22, GP-TM-25, GP-TM-27, GP-TM-29, GP-TM-33, GP-TM- 42, GP-TM-44, GP-TM-45
Secure Update Mechanism	GP-TM-05, GP-TM-06, GP-TM-18, GP-TM-19
Cybersecurity State Awareness	GP-TM-55, GP-TM-56

5.5.13.2 *Common Sections*

There are no common sections cross-referenced in the NIST document.

5.5.13.3 *Capability Analysis*

The following section compares the guidance in the current document to the selected 'Gold Standard'.

5.5.13.3.1 Logical / Physical Identifiers

5.5.13.3.1.1 Strengths

No strengths were identified during comparison to the gold standard document.

5.5.13.3.1.2 Weakness

No weaknesses were identified during comparison to the gold standard document.

5.5.13.3.1.3 Other Observations

The requirement of asset management as a policy does not have any additional guidance provided on how such a policy should be structured or implemented.

5.5.13.3.1.4 Capability Overview

Table 49 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 49: ENISA Logical / Physical Identifiers Summary

Strengths	Weaknesses	Other Observations
-	-	Additional guidance on good asset management practice

5.5.13.3.2 Secure Software Configuration

5.5.13.3.2.1 Strengths

When a device fails, it must revert to a known secure state of both upgrade failure and detected security breach.

5.5.13.3.2.2 Weakness

No weaknesses were identified during comparison to the gold standard document.

5.5.13.3.2.3 Other Observations

There is no guidance on what constitutes a security breach. There is also no mention as to the process of how breach (cybersecurity incident) detection occurs or its process.

5.5.13.3.2.4 Capability Overview

Table 50 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 50: ENISA Secure Software Configuration Summary

Strengths	Weaknesses	Other Observations
Known Good configuration Fallback	-	Manual vs. Automatic functions Ambiguous 'Security Breach'

5.5.13.3.3 Secure Data Storage & Transmission

5.5.13.3.3.1 Strengths

Devices should use proven solutions for cryptography and avoid any proprietary solutions; instead, utilise open standards that allow for interoperability. This cryptographic requirement is coupled with a list of reference documents. In conjunction, these proven solutions should be used to perform other functions requiring cryptography – for example, code signing, hashing, encrypting credentials and secure data transmission. To aid in this, devices should have some form of secure hardware storage or hardware secure processor.

When storing credentials locally on a device, ensure that they also include a salt (a random addition). It could perhaps explicitly state that no password should ever be stored in plain text (Lopez & Wu, 2015). Physical security of IoT is a newer issue as the devices can be geospatially separated. Ensuring that tamper-evident containers and device design prevents easy storage removal are considerations.

Data in transit should use 'state of the art protocols', such as TLS.

5.5.13.3.3.2 Weaknesses

The brief mention of "*Protection against local and physical attacks can be covered via functional security*" (ENISA, p. 82) does not provide any clarity or additional information on implementation.

The signing of install and code packages is covered in the same section of the document as runtime protections that prevent code hijacking – these two protection mechanisms differ significantly in technologies and approach.

The physical security of a device is equated to be encryption of data at rest. Secure management of cryptographic keys is mentioned without any additional guidance, only that it should be performed.

State of the art encryption is a subjective requirement, and there is no mention of the newer protocols, like DTLS. It also fails to mention to not use depreciated or known vulnerable versions of protocols.

5.5.13.3.3.3 Other Observations

The avoidance of proprietary and custom cryptography is mentioned but likened to 'in-house' creation. This could possibly fall under the umbrella of 'do not use custom cryptography' but is left open to interpretation when it should be explicitly disallowed. There is no mention of additional guidance specific to cryptography, e.g. The Federal Information Processing Standard (FIPS) from NIST. IoT devices are certainly not guaranteed to have secure hardware storage and secure hardware processors to handle advanced security functions. Privacy and transparency of data usage is a good policy to have; however, it is presented as a technical security measure, of which a policy is not.

5.5.13.3.3.4 Capability Overview

Table 51 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 51: ENISA Secure Data Storage & Transmission Summary

Strengths	Weaknesses	Other Observations
Use proven cryptography	-	No 'In house Development' warning No mention of FIPS
Hardware Secure Storage / Processor	Confusing 'Functional Security' Statement	IoT devices are not guaranteed to have this functionality
Cryptographically Sign Code	-	Signing code is not runtime protections
-		Data transparency
Physical Security	Conflation of encryption with physical security	
Encrypt Data at Rest & In-Transit	-	-
Secure Key Management	No additional information	-
'State of the Art' Protocols	No mention of not using Depreciated Versions	

5.5.13.3.4 Secure Interface Management

5.5.13.3.4.1 Strengths

Secure by default, is the current best practice approach to interface management (Lipner, 2004). This can include unique passwords per device and requiring these passwords to be changed during setup or provisioning. Protection against 'brute-force' logins may also involve interface management.

Applying the Principle of Least Privilege to all aspects of running programs and user actions creates a workload and management overhead, both during initial configuration and ongoing management and enforcement.

Physical removal of unneeded (e.g., USB) or debug ports (e.g., JTAG, named after the Joint Test Action Group) from the device will help limit the attack surface. If it is not possible to remove an access port, the port must be secured in line with all other management interfaces.

Always verify data received, and do not trust unknown devices. Incoming connections should not be allowed, and any not-in-use logical interfaces or network connections should be disabled.

5.5.13.3.4.2 Weakness

With security by default as described, this relies on manufacturers to implement protections, which leads to differing protection and quality levels. This work also ties into the prescribed unique and hard to crack device passwords that are without specific guidance. This lack of specific guidance results in open interpretation of what constitutes a 'unique password'.

A device's trust and discovery mechanisms are complicated by the many network types used in IoT, and not all network types are suitable to distrusting nodes at the protocol layer, requiring additional tooling.

5.5.13.3.4.3 Other Observations

A threat model should back the design of any authentication and authorization schema; however, this will rely on device level support, which may hamper this approach.

5.5.13.3.4.4 Capability Overview

Table 52 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 52: ENISA Secure Interface Management Summary

Strengths	Weaknesses	Other Observations
Security by Default	Variable Vendor Competence	Authentication & Authorization limited by device capabilities
Principle of Least Privilege	-	-
Physical Interface Remove	-	-
Disable Unneeded Interfaces	-	-
Verify all Network Data	Additional Tooling may be Required	-

5.5.13.3.5 Secure Update Mechanism

5.5.13.3.5.1 Strengths

The operating system must ensure that software and other programs can only be installed by authorized persons. This restriction should also include the ability to roll back to a known secure state, including the firmware of a device.

Automated updates from a trusted, secure source should be delivered by an Over-The-Air (OTA) mechanism and include a code verification check before any update occurs.

5.5.13.3.5.2 Weakness

No weaknesses were identified during comparison to the gold standard document.

5.5.13.3.5.3 Other Observations

No other observations were made during comparison to the gold standard document.

Capability Overview

Table 53 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 53: ENISA Secure Update Mechanism Summary

Strengths	Weaknesses	Other Observations
Program Installation Restrictions	-	-
Update Code Integrity	-	-
Configuration Rollback	-	-

5.5.13.3.6 Cybersecurity State Awareness

5.5.13.3.6.1 Strengths

The existence of a comprehensive logging system covering user authentication, accounts management, access rights, modifications to security rules, and general system functions. These logs should be monitored regularly to ensure that any malware or integrity errors are remedied.

5.5.13.3.6.2 Weakness

The description of logging fails to consider the limited storage of IoT devices. Centralised logging usually requires a dedicated Security Information and Event Management (SIEM) system – there is no mention of such dedicated logging, monitoring systems, or additional hardware.

5.5.13.3.6.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.13.3.6.4 Capability Overview

Table 54 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 54: ENISA Cybersecurity State Awareness Summary

Strengths	Weaknesses	Other Observations
Logging	No mentioned of SIEM / Centralized Log Storage	-

5.5.13.4 *Overall Summary Table: ENISA*

Table 55 is a summary of all identified strengths, weaknesses and other notes gathered from the ENISA document.

Table 55: ENISA Overall Summary

Baseline Capability	Strengths	Weaknesses	Other Observations
Logical / Physical Identifiers	-	-	Additional guidance on Asset Management
Secure Software Configuration	Known Good configuration Fallback	-	Manual vs. Automatic functions Ambiguous 'Security Breach'
Secure Data Storage & Transmission	Use proven cryptography	-	No 'In house Development' warning No mention of FIPS
	Hardware Secure Storage / Processor	Confusing 'Functional Security' Statement	IoT devices are not guaranteed to have this functionality
	Cryptographically Sign Code	-	Signing code is not runtime protections
	-	-	Data transparency

	Physical Security	Conflation of encryption with physical security	-
	Encrypt Data at Rest & In-Transit	-	-
	Secure Key Management	No additional information	-
	‘State of the Art’ Protocols	No mention of not using Depreciated Versions	-
Secure Interface Management	Security by Default	Variable Vendor Competence	Authentication & Authorization limited by device capabilities
	Principle of Least Privilege	-	-
	Physical Interface Remove	-	-
	Disable Unneeded Interfaces	-	-
	Verify all Network Data	Additional Tooling may be Required	-
Secure Update Mechanism	Program Installation Restrictions	-	-
	Update Code Integrity	-	-
	Configuration Rollback	-	-
Cybersecurity State Awareness	Logging	No mentioned of SIEM / Centralized Log Storage	-

5.5.14 Document Overview: ETSI

The current document under analysis against the gold standard is The European Telecommunications Standards Institute (ETSI), Baseline security recommendations for IoT in the context of critical information infrastructures. (ETSI, 2017).

5.5.14.1 *Capability to Section Mappings*

Table 56 details the sections of each reviewed document as they relate to the NIST ‘Security Capabilities’ described in the “IoT Device Cybersecurity Capability Core Baseline”. This document (ETSI) is not prescribed in all capabilities, denoted by a ‘-‘.

Table 56: ETSI Document to NIST Document Mappings

Baseline Capability (NIST)	SECTION (ETSI)
Logical / Physical Identifiers	-
Secure Software Configuration	-

Secure Data Storage & Transmission	4.4-1, 4.5-1, 4.5-2, 4.11-1, 4.11-2, 4.11-3
Secure Interface Management	4.1-1, 4.4-1, 4.6-1, 4.6-2
Secure Update Mechanism	4.3-1, 4.3-2, 4.3-7
Cybersecurity State Awareness	4.7-2, 4.10-1

5.5.14.2 *Common Sections*

5.5.14.2.1 ETSI: 4.4-1: Credentials and security-sensitive data shall be stored securely within services and on devices.

5.5.14.2.1.1 Strengths

Do not allow hard-coded credentials in software unless stored in hardware-backed secure storage such as a Trusted Execution Environment (TEE) or similar – such as a Universal Integrated Circuit Card UICC/embedded Universal Integrated Circuit Card (eUICC).

5.5.14.2.1.2 Weaknesses

No weaknesses were identified during comparison to the gold standard document.

5.5.14.2.1.3 Other Observations

There is a limited mention of obfuscation being trivially broken and not an effective means of code protection, and that reverse-engineering of a binary can occur.

5.5.14.2.1.4 Common Sections Overview

Table 57 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 57: ETSI Common Sections Summary

Strengths	Weaknesses	Other Observations
Hardware Backed Secure Storage	-	Obfuscation & reverse engineering mentioned

5.5.14.3 *Capability Analysis*

The following section compares the guidance in the current document to the selected 'Gold Standard'.

5.5.14.3.1 Logical / Physical Identifiers

This section is not cross-referenced in the NIST Document.

5.5.14.4 *Secure Software Configuration*

This section is not cross-referenced in the NIST Document.

5.5.14.5 *Secure Data Storage & Transmission*

See ETSI: 4.4-1: Credentials and security-sensitive data shall be stored securely within services and on devices.

5.5.14.5.1.1 Strengths

The usage and storage of any security sensitive data, including cryptographic keys or remote management and control traffic, should be encrypted at rest and in transit with the associated passphrase and access keys managed securely.

5.5.14.5.1.2 Weaknesses

Security sensitive data is broad and open to interpretation outside of a few specific examples.

5.5.14.5.1.3 Other Observations

Consumers should have the clear, informed ability to delete their personal data from both device and associated cloud or application services to facilitate device transfer, service cancellation or device disposal. Any of these actions should notify the consumer of success.

5.5.14.5.2 Capability Overview

Table 58 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 58: ETSI Secure Data Storage & Transmission Summary

Strengths	Weaknesses	Other Observations
Secure Storage & Management of Data & Keys	Security Sensitive Data is potentially unclear	-
-	-	Consumer data management

5.5.14.5.3 Secure Interface Management

See ETSI: 4.4-1: Credentials and security-sensitive data shall be stored securely within services and on devices.

5.5.14.5.3.1 Strengths

All IoT devices should be void of any shared or universal password or passphrase. The devices should also have un-needed hardware ports removed if possible, and any logical interfaces disabled if unneeded.

5.5.14.5.3.2 Weaknesses

No weaknesses were identified during comparison to the gold standard document.

5.5.14.5.3.3 Other Observations

Some of these capabilities are written as denied actions ('blacklist') instead of permitted actions ('whitelist').

5.5.14.5.4 Capability Overview

Table 59 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 59: ETSI Secure Interface Management Summary

Strengths	Weaknesses	Other Observations
Unique Device Passwords	-	-
Limit Hardware & Software Attack Surface	-	-
-	-	Some capabilities contain blacklisting language

5.5.14.6 *Secure Update Mechanism*

5.5.14.6.1.1 Strengths

All software components of an IoT device are to be updatable in a secure manner. This update mechanism should include a notification system for consumers to be aware of required updates.

5.5.14.6.1.2 Weaknesses

The guidance fails to mention code signing or other software verification measures. External resources references are not utilised to cover this deficiency.

5.5.14.6.1.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.14.6.1.4 Capability Overview

Table 60 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 60: ETSI Secure Update Mechanism Summary

Strengths	Weaknesses	Other Observations
Software Secure Updates	No mentions of software integrity	-
-	Inadequate usage of externally referenced documentation	-

5.5.14.7 *Cybersecurity State Awareness*

5.5.14.7.1.1 Strengths

Unauthorized changes to software should trigger an alert either to the consumer or administrator and cause the device to disconnect from all networks not a part of the alerting requirements. If an IoT device provides logging or telemetry data, this should be examined for cybersecurity purposes when such an alert is received.

5.5.14.7.1.2 Weaknesses

No weaknesses were identified during comparison to the gold standard document.

5.5.14.7.1.3 Other Observations

Provisions in this section are multi-part and contain aspects that should have been split out into a separate capability. For example, alerting and triggered network disconnection are not immediately relevant to the ability to restore to a known good state.

5.5.14.7.1.4 Capability Overview

Table 61 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 61: ETSI Cybersecurity State Awareness Summary

Strengths	Weaknesses	Other Observations
Software Change Monitoring & Alerting	-	-
-	-	Lack of granularity in provisions
Telemetry/Logging Analysis	-	-

5.5.14.8 *Overall Summary Table: ETSI*

Table 62 is a summary of all identified strengths, weaknesses and other notes gathered from the ETSI document.

Table 62: ETSA Overall Summary

Baseline Capability	Strengths	Weaknesses	Other Observations
Secure Data Storage & Transmission	Secure Storage & Management of Data & Keys	Security Sensitive Data is potentially unclear	-
	-	-	Consumer data management
	Hardware Backed Secure Storage		Obfuscation & reverse engineering mentioned
Secure Interface Management	Unique Device Passwords	-	-
	Limit Hardware & Software Attack Surface	-	-
	-	-	Some capabilities contain 'blacklisting' language
Secure Update Mechanism	Software Secure Updates	No mentions of software security	-
	-	Inadequate usage of externally referenced documentation	-
Cybersecurity State Awareness	Software Change Monitoring & Alerting	-	-
	-	-	Lack of granularity in provisions
	Telemetry/Logging Analysis	-	-

5.5.15 Document Overview: GSMA

The current document under analysis against the gold standard is the Global System for Mobile Communications Association (GSMA), Official Document CLP.11 – IoT Security Guidelines Overview Document Version 2.0.

5.5.15.1 *Capabilities to Section Mappings*

Table 63 details the sections of each reviewed document as they relate to the NIST 'Security Capabilities' described in the "IoT Device Cybersecurity Capability Core Baseline". This document (GSMA) is not prescribed in all capabilities, denoted by a '-'.

Table 63: GSMA Document to NIST Document Mappings

Baseline Capability (NIST)	SECTION (GSMA)
Logical / Physical Identifiers	CLP13_6.6.2, 6.8.1, 6.20.1
Secure Software Configuration	-
Secure Data Storage & Transmission	CLP13_6.4.1.1, 6.11, 6.12.1.1, 6.19, 7.6.1, 8.10.1.1, 8.11.1
Secure Interface Management	CLP13_6.9.1, 6.12.1, 6.20.1, 7.6.1, 8.2.1, 8.4.1
Secure Update Mechanism	7.5.1
Cybersecurity State Awareness	CLP13_6.13.1, 7.2.1, 9.1.1.2

The GSMA document specifies many terms; however, two notable ones are utilised in conjunction with unique identifiers: the Trusted Computing Base (TCB) and Generic Bootstrapping Architecture (GBA). A TCB is defined as "Hardware, software, and protocols that ensures the integrity of the Endpoint, performs mutual authentication with network peers, and manages communications and application security" (IoT Security Guidelines Endpoint Ecosystem V2.0, 2017, p. 26). This definition is broad-reaching and implies the existence and utilisation of hardware level secure storage and cryptography.

The GBA is paired with the Generic Authentication Architecture (GAA) to provide similar functionality as a desktop computer's TPM. It is defined by the Third Generation Partnership Project (*3GPP TS 33.220 V16.1.0*, 3GPP) as the ability to "…bootstrap authentication and key agreement for application security". This subset of functionality would usually form part of a TCB – which itself is also similar in function to a TPM, though not identical.

This reference is part of a conglomerate of different reports and is made up of different documents, of which the CLP*XX* denotes the specific document. CLP13 is the document considering *IoT Security Guidelines for EndPoints* (IoT Security Guidelines Endpoint Ecosystem V2.0, 2017). It does not contain a section 6.6.2, only a 6.6.1 and a 6.6. Taking a logical match of the Logical/Physical identifiers capability and the associated heading content, this is presumed to be a typo and associated to CLP13, 6.6.1 and not 6.6.2.

5.5.15.2 *Common Sections*

5.5.15.2.1 GSMA Section 6.12: Remote Endpoint Administration

5.5.15.2.1.1 Strengths

Administration of remote endpoints should, not store keys or credential in insecure storage, use unique keys or credentials per endpoint, enforcement a password policy, use MFA, have administrative access notifications, separate communication channels for management vs. operations and use current industry secure protocols.

5.5.15.2.1.2 Weaknesses

The usage of a password policy does not expand on acceptable guidelines for a password policy; for example, the current best practice is to use passphrases instead of arbitrarily complex passwords. The overhead of the prescribed security measures is not mentioned.

5.5.15.2.1.3 Other Observations

The further provision to use only the latest version of a given protocol with no publicly known exploits would strengthen the industry standard protocols guidance.

5.5.15.2.2 Common Section Overview

Table 64 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 64: GSMA Common Section 6.12 Summary

Strengths	Weaknesses	Other Observations
Separation of Managerial / Standard Communications	Lack of guidance on password policies	-
Stronger Administrative Authentication	-	MFA/2FA can cause overheads
-	-	Enhancement of the protocol guidance to latest version, with no known public vulnerabilities

5.5.15.3 *Capability Analysis*

The following section compares the guidance in the current document to the selected ‘Gold Standard’.

5.5.15.3.1 Logical / Physical Identifiers

5.5.15.3.1.1 Strengths

The provisioning specifications make specific use of mobile-centric technologies that are endemic to the GSMA's Industry sector. The specific technologies cover using unique cryptographic keys, cryptographic signing of unique keys, utilisation of the 'Trust Anchor' (analogous to Hardware Secure Storage) and strong integration into backend device management systems, specialised to GSM communications. This allows for unique provisioning and utility functions specific to this industry area, such as distinguishing active and deactivated devices, customer-based network links and devices, and monitoring these endpoints for security purposes.

5.5.15.3.1.2 *Weaknesses*

The protections specific are heavily reliant on industry specific functions that require specific tooling, processes, procedures, and device support.

5.5.15.3.1.3 Other Observations

The overhead to have the specified provisioning process occur per device is potentially significant.

5.5.15.3.1.4 Capability Overview

Table 65 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 65: GSMA Logical / Physical Identifiers Summary

Strengths	Weaknesses	Other Observations
Detailed Steps & Requirements for Cryptographic Identification	Industry-Specific Tooling	Potentially significant overhead

5.5.15.3.2 Secure Software Configuration

This section is not cross-referenced in the NIST Document.

5.5.15.3.3 Secure Data Storage & Transmission

See Common Section 6.12: Remote Endpoint Administration in addition.

5.5.15.3.3.1 Strengths

Data access should occur through an API for any hardware-backed secure storage (via the TCB) and should not be a direct read/write operation to ensure data integrity. The TCB should perform functions such as signature verification, key exchanges, encryption/decryption, message signing, message padding, and confirmation of confidentiality and integrity of the connection between TCB and application(s). All applications not a part of the CPU firmware or electrically erasable programmable read-only memory (EEPROM) should run in a restricted sandbox without full access to the device.

Communications between devices should authenticate any peer devices, connections, and use the latest available protocols.

5.5.15.3.3.2 Weaknesses

The TCB represents a single point of failure and provides all cryptographic functionality. This is specific to the GSMA outlook of IoT, and it is not representative of most software or hardware, where cryptographic functions can be performed outside of a trusted zone.

5.5.15.3.3.3 Other Observations

A selection of other documents published by the GSMA are listed as supplemental material regarding the TCB and its functions.

The specification of the latest version of protocols was only specified at the end of information on secure communications.

5.5.15.3.3.4 Capability Overview

Table 65 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 66: GSMA Secure Data Storage & Transmission Summary

Strengths	Weaknesses	Other Observations
API Usage for TCB/Hardware Secure Storage	-	-
TCB to Perform all Cryptographic Functions	Single Point of Failure Not Representative of the majority of current software systems	-
-	-	List of industry specific supplemental documents
Separation of Managerial / Standard Communications	-	-
Stronger Administrative Auth	-	MFA/2FA can cause overheads

Latest Protocol Versions	-	Placed at end of document, better served at start of document
End User Notifications	-	-

5.5.15.3.4 Secure Interface Management

See GSMA Section 6.12: Remote Endpoint Administration in addition.

5.5.15.3.4.1 Strengths

Endpoints must employ some form of password management. This password management system should include brute-force attack mitigations, disable hardcoded passwords, ensure user credentials are not displayed during login and enforce a form of login back-off for invalid attempts (which forms part of brute-force protections). Cryptographically signed endpoints must also be able to prove that they are the true owner of a signed secret by way of PKI keys that a backend management system can verify.

The device should have all hardware or software debugging, testing, and diagnostic interfaces removed. Examples of possible interfaces are provided.

IoT devices that incorporate rich displays of some type (e.g., touchscreens) must be able to display both alerts and user interaction prompts. An alert should cover security and information related events like physical tampering, while migration of the device via an action should require user approval.

5.5.15.3.4.2 Weaknesses

The proof of signed endpoints relies heavily on backend management systems. The description of 'Password best practice enforcement' does not provide additional information or clarity.

5.5.15.3.4.3 Other Observations

Some capabilities of password enforcement may rely on backend authentication systems. The section on protocol and potential identify spoofing is informative but lacks actionable guidance.

5.5.15.3.4.4 Capability Overview

Table 67 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 67: GSMA Secure Interface Management Summary

Strengths	Weaknesses	Other Observations
Password Management & Protections	'Best Practise' capability is unhelpful and vague	May rely on backend authentication system support
Cryptographic Proof of Identity	Relies heavily on backend systems	-
-	-	Information on spoofing, but no new prevention/protections that have not already been prescribed
Remove Unused Interfaces	-	-
User Alerting	-	-
User Interactions	-	-

5.5.15.3.5 Secure Update Mechanism

5.5.15.3.5.1 Strengths

Over-The-Air (OTA) Updates should allow for the graceful recovery of a failed update, cryptographic signing, verification of update files, and be delivered via secure communications.

5.5.15.3.5.2 Weaknesses

No weaknesses were identified during comparison to the gold standard document.

5.5.15.3.5.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.15.3.5.4 Capability Overview

Table 68 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 68: GSMA Secure Update Mechanism Summary

Strengths	Weaknesses	Other Observations
Resilient & Cryptographically Secure OTA Updates	-	-

5.5.15.3.6 Cybersecurity State Awareness

5.5.15.3.6.1 Strengths

Logging should incorporate device environment and diagnostics data as well as application, system, and kernel logs. These logs should be ingested into a SIEM to allow for anomaly detection. A stated low priority recommendation is to beware of unintentional (or intentional) denial of service of all radio communications, not just communication channels due to traffic bursts or external interference.

5.5.15.3.6.2 Weaknesses

No weaknesses were identified during comparison to the gold standard document.

5.5.15.3.6.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.15.3.6.4 Capability Overview

Table 69 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 69: GSMA Cybersecurity State Awareness Summary

Strengths	Weaknesses	Other Observations
Logging & Diagnostic Data	-	-
Anomaly Detection	-	-
DoS Awareness	-	All wireless communications, not just data or management

5.5.15.4 *Overall Summary Table: GSMA*

Table 70 is a summary of all identified strengths, weaknesses and other notes gathered from the GSMA document.

Table 70: GSMA Overall Summary

Baseline Capability	Strengths	Weaknesses	Other Observations
Logical / Physical Identifiers	Detailed Steps & Requirements for Cryptographic Identification	Industry Specific Tooling	Potentially significant overhead
Secure Data Storage and Transmission	API Usage for TCB/Hardware Secure Storage	-	-
	TCB to Perform all Cryptographic Functions	Single Point of Failure Not Representative of most software systems	-

	-	-	List of industry specific supplemental documents
	Separation of Managerial / Standard Communications	Lack of guidance on password policies	-
	Stronger Administrative Authentication	-	MFA/2FA can cause overheads
	-	-	Enhancement of the protocol guidance to latest version, with no known public vulnerabilities
	Latest Protocol Versions	-	Placed at end of document, better served at start of document
	End User Notifications	-	-
Secure Interface Management	Password Management & Protections	'Best Practise' capability is unhelpful and vague	May rely on backend authentication system support
	Cryptographic Proof of Identity	Relies heavily on backend systems	-
	-	-	Information on spoofing, but no new prevention / protections that have not already been prescribed
	Remove Unused Interfaces	-	-
	User Alerting	-	-
	User Interactions	-	-
Secure Update Mechanism	Resilient & Cryptographically Secure OTA Updates	-	-
Cybersecurity State Awareness	Logging & Diagnostic Data	-	-
	Anomaly Detection	-	-
	DoS Awareness	-	All wireless communications, not just data or management

5.5.16 Document Overview: IEC

The current document under analysis against the gold standard is the International Electrotechnical Commission (IEC), IEC 62443-4-2, Edition 1.0, Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components (IEC 62443-4-2, 2019).

5.5.16.1 *Capabilities to Section Mappings*

Table 71 details the sections of each reviewed document as they relate to the NIST 'Security Capabilities' described in the "IoT Device Cybersecurity Capability Core Baseline".

Table 71: IEC Document to NIST Document Mappings

Baseline Capability (NIST)	SECTION (IEC)
Logical / Physical Identifiers	CR 1.2
Secure Software Configuration	CR 7.4, CR 7.6
Secure Data Storage & Transmission	CR 3.1, CR 3.4, CR 4.1, CR 4.2, CR 4.3
Secure Interface Management	CR 1.1, CR 1.2, CR 1.5, CR 1.7, CR 1.11, CR 2.1, CR 2.2, CR 2.13, CR 7.7, EDR 2.13
Secure Update Mechanism	CR 3.4, EDR 3.10
Cybersecurity State Awareness	CR 2.8, CR 3.9, CR 6.1, CR 6.2

5.5.16.2 *Common Sections*

5.5.16.2.1 IEC: CR 1.2: Software Process and Device Identification and Authentication

5.5.16.2.1.1 Strengths

All IoT devices and users should be uniquely identifiable and authenticatable.

5.5.16.2.1.2 Weaknesses

The unique identification and authorization mechanism depends on the existence of a corresponding unique identifier; however, there is no guidance on what is acceptable for usage as a unique identifier.

5.5.16.2.1.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.16.2.2 IEC: CR 3.4: Software Information Integrity

5.5.16.2.2.1 Strengths

Software should incorporate the ability to perform authenticity checks on both software and configuration. Each individual software component should also be capable of notification when detecting an unauthorized change attempt. These mechanisms should utilize formal checks, for example, cryptographic hashes.

5.5.16.2.2.2 Weaknesses

No weaknesses where identified during comparison to the gold standard document.

5.5.16.2.2.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.16.2.3 Common Section Overview

Table 72 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 72: IEC Common Section Summary

Strengths	Weaknesses	Other Observations
Software Verification Checks	-	-
Unique Identifiers	No guidance on acceptable unique identifiers	-

5.5.16.3 *Capability Analysis*

The following section compares the guidance in the current document to the selected 'Gold Standard'.

5.5.16.3.1 Logical / Physical Identifiers

See IEC: CR 1.2: Software Process and Device Identification and Authentication in addition.

5.5.16.3.2 Secure Software Configuration

5.5.16.3.2.1 Strengths

All individual components of an IoT device should be able to reconfigure themselves and recover to a known secure state. This known secure state should include patches, configuration options, documentation, and testing procedures.

5.5.16.3.2.2 Weaknesses

The network configuration and specifications thereof are offloaded to the manufacturer, with the only listed requirements that configuration can occur and that there is an interface of some type to allow this configuration. Automated monitoring is also bundled into this capability, requiring a machine-readable listing of a device's current configuration – machine readable is not always synonymous with human readable.

5.5.16.3.2.3 Other Observations

Secure recovery is a device-specific aspect as this capability also combines documentation and operational processes into the device recovery aspect. This expands the scope of work required from a single device to device and its associated areas, which will vary from organisation to organisation.

5.5.16.3.2.4 Capability Overview

Table 73 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 73: IEC Secure Software Configuration Overview

Strengths	Weaknesses	Other Observations
Component Level Known Secure Recovery	-	Device specific & complicated Expansion to include process & documentation
Network Security Configurations	Offloaded to supplier/manufacturer	-

5.5.16.3.3 Secure Data Storage & Transmission

See IEC: CR 3.4: Software Information Integrity in addition.

5.5.16.3.3.1 Strengths

All communication should be verified for the authenticity of the payload and the sender. The additional verification guidance focuses on altering the network connection type to ensure that the integrity of data is not adversely affected by the environmental circumstances of a device.

Data confidentiality prescribes protective measures for both data at rest and data in transit. Data at rest protections should include explicit authorization for data access. This protection should also include the ability to erase all data due to device decommissioning or transfer, congruent to a device reset.

All cryptographic functions should use secure, well-known functions. Additional links to external documents such as FIPS 140-2 Security Requirements for Cryptographic Modules (National Institute of Standards and Technology, 2019) and clarify the allowed algorithms and versions that should be put into service.

5.5.16.3.3.2 Weaknesses

The brief explanation that you can verify both integrity and authentication without providing confidentiality is not explained further. The possible external influences on device and data decommissioning are not brought to awareness.

5.5.16.3.3.3 Other Observations

Some additional guidance on what data should be protected would enhance the provided guidelines. Cryptography is listed as if required – this is counterintuitive to most cybersecurity functions.

5.5.16.3.3.4 Capability Section Overview

Table 74 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 74: IEC Secure Data Storage & Transmission

Strengths	Weaknesses	Other Observations
Data Protection in Transit & at Rest	-	Additional notes on what data should be secured would be beneficial
Integrity & Authenticity of Data	Lack of Confidentiality is a side note	-
Data Erasure	No mention of potential Regulatory Influences	-
Use Cryptography	-	Listed as 'If Required'

5.5.16.3.4 Secure Interface Management

5.5.16.3.4.1 Strengths

All devices must implement secure user authentication and authorization. This authorisation is also to include segregation of duties and can be enforced either locally, or by integration into a management system. This enforcement of user restrictions is best combined with the ability for software or hardware components to identify and authenticate between themselves. These operations should be backed by a standard and secure mechanism, like X.509 Certificates, GUIDs or user accounts that can be associated with an identity. If passwords must be used, then they should allow for configurable complexity enforcement, with some form of brute-force back-off. The usage of wireless network interfaces should be restricted and integrated into any monitoring systems.

5.5.16.3.4.2 Weaknesses

Wireless communications restrictions, according to best industry practice, is not expanded to provide clarity on the required actions.

5.5.16.3.4.3 Other Observations

Expanding wireless restrictions to include monitoring for rogue access points or wireless activity is a potential legal issue.

5.5.16.3.4.4 Capability Section Overview

Table 75 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 75: IEC Secure interface Management Summary

Strengths	Weaknesses	Other Observations
User Identification	-	-
Secure User/Human Authentication	-	-
Secure Machine/Component Authentication	-	-
Wireless Networking Restrictions	Industry Best Practise Dedicated Rogue AP detection	Potential Legalities
Principle of Least Functionality	-	-

Restrict Physical Access to Test/Debug Interfaces	-	-

5.5.16.3.5 Secure Update Mechanism

5.5.16.3.5.1 Strengths

Remote installation of patches, updates, and upgrades must occur over a secure channel using a verified update file. This secure channel is to account for a device's networking interface and the associated changes in the delivery mechanism.

5.5.16.3.5.2 Weaknesses

No weaknesses were identified during comparison to the gold standard document.

5.5.16.3.5.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.16.3.5.4 Capability Section Overview

Table 76 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 76: IEC Secure Update Mechanism Summary

Strengths	Weaknesses	Other Observations
Secure Updates	-	-

5.5.16.3.6 Cybersecurity State Awareness

5.5.16.3.6.1 Strengths

An auditable log of events should be kept on an IoT device. These events should be kept for multiple categories, such as configuration changes, request errors, control system actions, backend restoration, and access control. Each event should include appropriate timeline-based reconstruction and identification information such as a timestamp, source, unique event ID, event result or action, category, and type. These logs would ideally be monitored continuously via a SIEM. The logs and associated tools should also be immutable and protected from modification, access, or deletion by anyone but authorized administrators.

5.5.16.3.6.2 Weaknesses

Audit logs are to be protected against unauthorized modification, but tools and components are to allow read-only access. If administrators are permitted to modify the audit log as part of normal duties, then the prescription that authorized humans or tools are to have read-only access should be clarified or joined with the preceding argument – that authorized administrative tools and users are to have full access, and non-administrator, authorized users can have read-only access.

5.5.16.3.6.3 Other Observations

The brief notice that security-related events can only be captured if the functionality exists within a component and that all events that exist within the prescribed categories be captured is not immediately clear as to its purpose. If a device does not generate logs, then it is impossible to capture them, and capturing all events possible is the industry standard default, relaxing as unneeded events are identified. The storage of audit logs on hardware-enforced write-once media is different to most existing hardware - most portable or universal storage media is not write-once hardware-enforced media, creating a dependency on specialised hardware.

5.5.16.3.6.4 Capability Overview

Table 77 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 77: IEC Cybersecurity State Awareness Summary

Strengths	Weaknesses	Other Observations
Detailed Audit Logging	Conflicting access guidance	Unnecessary clarifications Non-Default capture all events Write-Once media usage

5.5.16.3.7 Overall Summary Table: IEC

Table 78 is a summary of all identified strengths, weaknesses and other notes gathered from the IEC document.

Table 78: IEC Overall Summary

Baseline Capability	Strengths	Weaknesses	Other Observations
Secure Update Mechanism	Software Verification Checks	-	-
Logical / Physical Identifiers	Unique Identifiers	No guidance on what a good unique identifier is	-

Secure Software Configuration	Component Level Known Secure Recovery	-	Device-specific & complicated Expansion to include process & documentation
	Network Security Configurations	Offloaded to supplier/manufacturer	-
Secure Data Storage and Transmission	Data Protection in Transit & at Rest	-	Additional notes on what data should be secured would be beneficial
	Integrity & Authenticity of Data	Lack of Confidentiality is a side note	-
	Data Erasure	No mention of potential Regulatory Influences	-
	Use Cryptography	-	Listed as 'If Required'
Secure Interface Management	User Identification	-	-
	Secure User/Human Authentication	-	-
	Secure Machine/Component Authentication	-	-
	Wireless Networking Restrictions	Industry Best Practise Dedicated Rogue AP detection	Potential Legalities
	Principle of Least Functionality	-	-
	Restrict Physical Access to Test/Debug Interfaces	-	-
Secure Update Mechanism	Secure Updates	-	-
Cybersecurity State Awareness	Detailed Audit Logging	Conflicting access guidance	Unnecessary clarifications Non-Default capture all events Write-Once media usage

5.5.17 Document Overview: IIC

The current document under analysis against the gold standard is the Industrial Internet Consortium (IIC), Industrial Internet of Things Volume G4: Security Framework.

5.5.17.1 *Capabilities to Section Mappings*

Table 79 details the sections of each reviewed document as they relate to the NIST 'Security Capabilities' described in the "IoT Device Cybersecurity Capability Core Baseline".

Table 79: IIC Document to NIST Document Mappings

Capability (NIST)	SECTION (IIC)
Logical / Physical Identifiers	7.3, 8.5, 11.7, 11.8
Secure Software Configuration	7.3, 7.6, 8.10, 11.5
Secure Data Storage & Transmission	7.3, 7.4, 7.6, 7.7, 8.8, 8.11, 8.13, 9.1, 10.4, 11.9
Secure Interface Management	7.3, 7.4, 8.3, 8.6, 11.7
Secure Update Mechanism	7.3, 11.5
Cybersecurity State Awareness	7.3, 7.5, 7.7, 8.9, 10.3, 10.4

5.5.17.2 *Common Sections*

The following sections are referenced multiple times in the NIST document:

- 7.3: Endpoint Protection
- 7.6: Security Configuration and Management
- 7.7: Data Protection
- 11.5: Endpoint Configuration and Management

5.5.17.2.1 IIC: 7.3: Endpoint Protection

5.5.17.2.1.1 Strengths

The requirements break an endpoint into multiple functional areas. These functional areas are; protections, physical security, root of trust, identity, integrity protection, access control, secure configuration management, monitoring and analysis, data protection, security modules, and policy.

This approach of broad categories and aspects of endpoint security (where a single device can have *N* endpoints) carries the added overhead of now needing to track both the purpose and function of all endpoints on a single device and apply security as required to each endpoint. Whilst this is not different from the traditional approach to cybersecurity when dealing with multiple services (with a service synonymous to an endpoint), it must be noted as raising the complexity of the capability, first by applying the listed capabilities to every end point and again when further additions are made in for further guidance.

5.5.17.2.1.2 Weaknesses

The provided scope of guidance also creates a variety of both purposes and functions of endpoints that must be tracked, creating potentially significant managerial overhead. The security measures provided require interpretation to implement, with many of the technical details obscured by the high level of discussion.

5.5.17.2.1.3 Other Observations

Later sections point out that security should not get in the way of operations and should be modular whenever possible to allow for the same protections to be rolled out and increase the overall security posture.

5.5.17.2.1.4 Section Overview

Table 80 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 80: IIC Common Section 7.3 Summary

Strengths	Weaknesses	Other Observations
Breadth of Security Measures	Purpose vs. Function Intermixed	Modular Security is a good goal, but much harder to do correctly

5.5.17.2.2 IIC: 7.6: Security Configuration and Management

The approach to secure software in this section is a part of a larger aspect of security and change management and describes a generic approach to cover most aspects of secure software management from a managerial perspective as opposed to a technical one. Given the target audience of this document, this makes for a decent starting point.

5.5.17.2.2.1 Strengths

The information is targeted as a managerial overview and presents the salient points to cover the required processes to support the outlined goals.

5.5.17.2.2.2 Weaknesses

There are no external references that can be used as an implementation guide, and the listed references are few.

5.5.17.2.2.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.17.2.2.4 Section Overview

Table 81 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 81: IIC Common Section 7.6 Summary

Strengths	Weaknesses	Other Observations
Overview of Process	Lack of more detailed external resources Incredibly Brief	-

5.5.17.2.3 IIC: 7.7: Data Protection

5.5.17.2.3.1 Strengths

Data is contextualised to its current location – at rest, in use or in motion. This is an important distinction to make and allows for finer-grained targeting of protections for differing data types and locations. All data should be protected against unauthorized access, uncontrolled changes, and the protections applied should be commensurate with the impact of data loss or falsification. This data should sit under a defined retention timeframe.

5.5.17.2.3.2 Weaknesses

The listed categories of controls are effectively useless – they simply list that isolation, replication, confidentiality, access, and integrity controls need to be applied to data. Without additional technical guidance, implementation of any protections will rely on interpretation.

5.5.17.2.3.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.17.2.3.4 Section Overview

Table 82 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 82: IIC Common Section 7.7 Summary

Strengths	Weaknesses	Other Observations
Data Location Contextualization	-	-
Categorical approach to data security	No Guidance on Controls	-

5.5.17.2.4 IIC: 11.5: Endpoint Configuration and Management

5.5.17.2.4.1 Strengths

Machine (device) policies, either set manually or enforced via device management systems, must be enforced correctly. This includes relevant sub controls and the applicability to any of the sub-components. This consists of three components – a human configurable policy, a parser and a configurator that applies the human configured policy. Access to any policy should be highly restricted.

5.5.17.2.4.2 Weaknesses

Provisions covering graphical user interface prompts for update or configuration confirmation are only mentioned briefly and without detail. The delivery mechanism for updates is also brief, mentioning that delivery of policy should occur over secure channels, without any additional detail. This lack of detail and brief mentions continues in reference to logging, auditing, and privacy concerns.

5.5.17.2.4.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.17.2.4.4 Section Overview

Table 83 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 83: IIC Common Section 11.5 Summary

Strengths	Weaknesses	Other Observations
Configurable Security Policies	Dearth of detail in all aspects	-

5.5.17.3 *Capability Analysis*

The following section compares the guidance in the current document to the selected 'Gold Standard'.

5.5.17.3.1 Logical / Physical Identifiers

See IIC: 7.3: Endpoint Protection in addition.

5.5.17.3.1.1 Strengths

Identity is described as a chain of trust that can be violated. This chain allows for clear levels of security that can be applied, with examples given. This approach is backed by external reference to international standards to bolster the provided guidance. The strong emphasis may overshadow other equality important cybersecurity areas.

5.5.17.3.1.2 Weaknesses

Identity management will introduce an overhead and require a level of operational and managerial maturity level to implement. The guidance provided to implement identity management requires extrasensory perception to perform, owing to the complete dearth of instruction.

5.5.17.3.1.3 Other Observations

The additional external references cover extensive areas of cybersecurity. Without any cross-referencing within the document to these external references, it generates additional questions. Levels of trust, sub-identity, component identity, and namespaces would benefit from internal document cross-referencing and external information. The ability for devices to be managed in the described process would require a SIEM.

5.5.17.3.1.4 Section Overview

Table 84 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 84: IIC Logical / Physical Identifiers Summary

Strengths	Weaknesses	Other Observations
Identity Management	Induced Overhead Requires maturity of process	-
-	-	Confusing supplementary concepts
External Standard References	-	Own outlook as to what IIoT is

-	-	Implicit SIEM requirement

5.5.17.3.2 Secure Software Configuration

See IIC: 7.3: Endpoint Protection in addition.

5.5.17.3.2.1 Strengths

Specific mentions that devices should be able to enforce individual policy settings for each component of a device.

5.5.17.3.2.2 Weaknesses

The assumption is made that the IoT device will support the required cryptographic functions and support integration into the required cryptographic key management system.

5.5.17.3.2.3 Other Observations

A GUI is not always present on IoT devices and as such, is perhaps best left as an optional layer of the CLI interface. The potential overheads for central management of policies can be significant.

5.5.17.3.2.4 Section Overview

Table 85 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 85: IIC Secure Software Configuration Summary

Strengths	Weaknesses	Other Observations
Secure Software management	-	-
-	Assumed IoT Device Capabilities Assumed IoT Integration Capabilities	-
Policy Enforcement	-	GUI assumed Potential Overhead

5.5.17.3.3 Secure Data Storage & Transmission

See IIC: 7.3: Endpoint Protection, IIC: 7.6: Security Configuration and Management and IIC: 7.7: Data Protection in addition.

5.5.17.3.3.1 Strengths

There is a differentiation between data at rest, in use and in motion. All cryptography is to be industry-tested and standardised, with key rollover on a timed basis. Seeds for cryptographic functions should come from hardware based random number generators (RNG) when possible. Security policies should have different monitoring levels dependent on data monitored and not obstruct normal operations.

5.5.17.3.3.2 Weaknesses

A lack of guidance when ascertaining where to apply cryptographic protections. A high level of assumed organisational, network infrastructure and process maturity to handle the overhead of managing the protections and implementing the required processes.

5.5.17.3.3.3 Other Observations

IoT device capabilities are assumed to have specified support for cryptography operations.

5.5.17.3.3.4 Section Overview

Table 86 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 86: IIC Secure Data Storage & Transmission Summary

Strengths	Weaknesses	Other Observations
Standardised Cryptography	Lack of Guidance on Data to Protect Network complexity for 'Security Metadata' Required Maturity Level for Security & organisation Overheads	Assumption of Device Capabilities
Targetable & Transparent Security Policies	-	-

5.5.17.3.4 Secure Interface Management

See IIC: 7.3: Endpoint Protection in addition.

5.5.17.3.4.1 Strengths

Physical security is an important part of IoT – it makes good use of existing external standards to supplement clear examples.

5.5.17.3.4.2 Weaknesses

The document is substantially longer than needed to present the information.

5.5.17.3.4.3 Other Observations

Hardware security modules are specialised and may not be present on all IoT devices.

5.5.17.3.4.4 Section Overview

Table 87 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 87: IIC Secure Interface Management Summary

Strengths	Weaknesses	Other Observations
Physical Security	-	Hardware security modules are not always present

5.5.17.3.5 Secure Update Mechanism

See IIC: 7.3: Endpoint Protection in addition.

5.5.17.3.5.1 Strengths

No strengths were identified during comparison to the gold standard document.

5.5.17.3.5.2 Weaknesses

Security policies and their operations are incorrectly equated to as forming a part of a secure update mechanism.

5.5.17.3.5.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.17.3.5.4 Section Overview

Table 88 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 88: IIC Secure Update Mechanism Summary

Strengths	Weaknesses	Other Observations
-	Security policy parser is not a secure update mechanism	-

5.5.17.3.6 Cybersecurity State Awareness

See IIC: 7.3: Endpoint Protection and IIC: 7.7: Data Protection in addition.

5.5.17.3.6.1 Strengths

Monitoring must be associated with alerting and action for the endpoints, their communications, secure remote logging, and the device's supply chain. Any data captured in this effort must be stored securely and accessible only by authorized personnel.

5.5.17.3.6.2 Weaknesses

Monitoring a supply chain is difficult when a single entity owns the entire chain – a supply chain comprised of multiple entities is significantly more difficult to monitor.

5.5.17.3.6.3 Other Observations

Monitoring of devices is listed as a required action but provides only broad categories of potential events to monitor.

5.5.17.3.6.4 Section Overview

Table 89 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 89: IIC Cybersecurity State Awareness Summary

Strengths	Weaknesses	Other Observations
Monitoring, Action & Alerts	-	What to monitor
-	Supply chain monitoring is difficult	-

5.5.17.4 *Overall Summary Table: IIC*

Table 90 is a summary of all identified strengths, weaknesses and other notes gathered from the IIC document.

Table 90: IIC Overall Summary

Baseline Capability	Strengths	Weaknesses	Other Observations
All	Breadth of Security Measures	Purpose vs. Function Intermixed	Modular Security is a good goal, but much harder to do correctly
Secure Software Configuration	Overview of Process	Lack of more detailed external resources Incredibly Brief	-

Secure Data Storage and Transmission	Data Location Contextualization	-	-
	Categorical approach to data security	No Guidance on Controls	-
Secure Software Configuration	Configurable Security Policies	Dearth of detail in all aspects	-
Logical / Physical Identifiers	Identity Management	Induced Overhead Requires maturity of process	-
	-	-	Confusing supplementary concepts
	External Standard References	-	Own Outlook to what IIoT is
	-	-	Implicit SIEM requirement
Secure Software Configuration	Secure Software management	-	-
	-	Assumed IoT Device Capabilities Assumed IoT Integration Capabilities	-
	Policy Enforcement	-	GUI assumed Potential Overhead
Secure Data Storage and Transmission	Standardised Cryptography	Lack of Guidance on Data to Protect Network complexity for 'Security Metadata' Required Maturity Level for Security & organisation Overheads	Assumption of Device Capabilities
	Targetable & Transparent Security Policies	-	-
Secure Interface Management	Physical Security	-	Hardware security modules are not always present
Secure Update Mechanism	-	Security policy parser is not a secure update mechanism.	-
Cybersecurity State Awareness	Monitoring, Action & Alerts	-	What to monitor
	-	Supply chain monitoring is difficult	-

5.5.18 Document Overview: IoTSF

The current document under analysis against the gold standard is The IoT Security Foundation (IoTSF), IoT Security Compliance Framework (IoT Security Compliance Framework, 2016).

5.5.18.1 *Capability to Section Mappings*

Table 91 details the sections of each reviewed document as they relate to the NIST 'Security Capabilities' described in the "IoT Device Cybersecurity Capability Core Baseline".

Table 91: IoTSF Document to NIST Document Mappings

Baseline Capability (NIST)	SECTION (IoTSF)
Logical / Physical Identifiers	2.4.8.1, 2.4.14.3, 2.4.14.4
Secure Software Configuration	2.4.8.17, 2.4.15
Secure Data Storage & Transmission	2.4.6.5, 2.4.7, 2.4.8.8, 2.4.8.16, 2.4.9, 2.4.12.2, 2.4.16.1, 2.4.16.2
Secure Interface Management	2.4.4.5, 2.4.4.9, 2.4.5.5, 2.4.6.3, 2.4.6.4, 2.4.7, 2.4.8
Secure Update Mechanism	2.4.5.1, 2.4.5.2, 2.4.5.3, 2.4.5.4, 2.4.5.8, 2.4.6.1
Cybersecurity State Awareness	2.4.7.5

5.5.18.2 *Common Sections*

The following section in the IoTSF document is referenced in multiple capabilities:

- 2.4.7 - Compliance Applicability – Device Wired and Wireless Interfaces

5.5.18.2.1 IoTSF: 2.4.7 - Compliance Applicability – Device Wired and Wireless Interfaces

5.5.18.2.1.1 Strengths

All network connections are to be restricted via a firewall on all interfaces. This firewall should have its configuration reviewed and documented to an accepted baseline secure state. If a device has bridged interfaces, these should be restricted or removed if possible. All unused communication ports should be closed. An unauthorised change should trigger both an alert and a complete network disconnect that requires manual intervention to return a device to a connected state.

If passkeys or passphrases are needed for a network connection, each device is to have a unique passkey or passphrase. If factory keys are present, they are changed or uniquely set by the manufacturer as a part of provisioning. When authenticating for the first time, strong authentication shall be used that requires human interaction with the device. On device reset, warn that security may be compromised due to configuration alteration.

Cryptography and protocol usage should use the latest protocol versions available; have no publicly known vulnerabilities, and secure storage of access keys should follow an industry standard.

The document states that Wi-Fi is to use WPA2-AES. Where TCP/UDP connections are used, the connection is to be secured by a D/TLS version that is the latest available and does not suffer from any publicly known vulnerabilities. All cipher suites are to be validated against a current industry standard, such as NIST 800-131A (Barker & Roginsky, 2019) or OWASP (*IoT Framework Assessment - OWASP*, 2016), with insecure ciphers removed. A device should continue to function if it is removed or disconnected from a network gracefully. When possible, the broadcast power of the wireless antennae is to be limited.

5.5.18.2.1.2 Weaknesses

The requirement of a secure state is ambiguous and relies on the assumption of contextual and technical knowledge.

5.5.18.2.1.3 Other Observations

There is a specific mention of validation cryptographic import or export requirements for a device and its association cryptographic capabilities, and that devices should be maintained throughout the lifetime of the device.

5.5.18.2.2 Common Section Overview

Table 92 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 92: IoTSF Common Section 2.4.7 Summary

Strengths	Weaknesses	Other Observations
Firewall & Network Restrictions	Ambiguous 'Secure State'	-
Up-To-Date Modern Cryptography	-	OWASP is not a conformance standard Import / Export Restrictions
Secure Protocol & Communications	-	-
Graceful Network Failures	-	-
-	-	Warning on device reset about security options
-	-	Device lifetime and support

5.5.18.3 *Capability Analysis*

The following section compares the guidance in the current document to the selected 'Gold Standard'.

5.5.18.3.1 Logical / Physical Identifiers

5.5.18.3.1.1 Strengths

Devices must contain a unique and tamper-resistance device identifier that is tied to the hardware. The manufacturer should log this identifier, so the duplicated devices can be identified and removed or destroyed.

5.5.18.3.1.2 Weaknesses

Reliance on the manufacturer to implement a secure hardware identifier.

5.5.18.3.1.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.18.3.1.4 Capability Summary

Table 93 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 93: IoTSF Logical / Physical Identifiers Summary

Strengths	Weaknesses	Other Observations
Manufacturer Hardware Identifier	Reliance on Manufacturer	-

5.5.18.3.2 Secure Software Configuration

5.5.18.3.2.1 Strengths

When protections are triggered, the device should have the capability to restore itself to a known secure state. Configuration changes via a web interface should prevent unauthorized changes to any potentially sensitive options. These configuration options should be provisionable from a just-in-time service.

5.5.18.3.2.2 Weaknesses

There is no guidance on what a constitutes a sensitive configuration option.

5.5.18.3.2.3 Other Observations

There is no explicit logging requirement mentioned; however, there are actions that imply the requirement of such a mechanism. The tracking of changed parameters and who is authorized to make changes to sensitive configuration options is one such example.

5.5.18.3.2.4 Capability Summary

Table 94 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 94: IoTSF Secure Software Configuration Summary

Strengths	Weaknesses	Other Observations
Restoration to a Known Good State	-	-
Secure Configuration	Ambiguous 'Sensitive Configuration Options'	Implicit audit logging
Just-In-Time Provisioning	-	-

5.5.18.3.3 Secure Data Storage & Transmission

See IoTSF: 2.4.7 - Compliance Applicability – Device Wired and Wireless Interfaces in addition.

5.5.18.3.3.1 Strengths

Passwords and other credentials should not be stored locally on a device. If they must be stored on a device, only the most privileged account can view these credentials. Cryptography compliant to an industry standard, such as NIST SP 800-63b (Grassi et al., 2017) or similar, should be used to encrypt stored passwords, and any ciphers with public vulnerabilities removed or disabled. The life cycle of the product concerning cryptographic capabilities should abide by NIST SP800-131A (Barker & Roginsky, 2019). If present, a hardware random number generator has been validated for true randomness using FIPS 140-2 (Evans, 2001), or a similar process should be used to generate all random numbers. Any cryptographic key provisioning should protect against key copying, and cryptographic keys should be stored in tamper-proof hardware secure storage.

All personal information is to be encrypted at rest and in transit. This personal information should be erasable on request from both devices and any registered services to facilitate the transfer or reset of the device the data is stored on.

5.5.18.3.3.2 Weaknesses

No weaknesses were identified during comparison to the gold standard document.

5.5.18.3.3.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.18.3.3.4 Capability Summary

Table 95 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 95: IoTSF Secure Data Storage & Transmission Summary

Strengths	Weaknesses	Other Observations
Secure Password Storage	-	-
Device Reset	-	-
Secure Key Management & Provisioning	-	-
Personal Data Management	-	-

5.5.18.3.4 Secure Interface Management

See IoTSF: 2.4.7 - Compliance Applicability – Device Wired and Wireless Interfaces in addition.

5.5.18.3.4.1 Strengths

As an alternative to removing JTAG or other similar debugging interfaces, ensure that these interfaces have authentication and authorization attached to them. If the ports cannot be physically removed, they should be physically isolated or inaccessible.

Remove all unneeded accounts from the system, including debug or testing accounts. These accounts should be documented and incorporated into an access control schema. When possible, unique identifiers should be physically stored on the device in a tamper-proof mechanism. All files, directories and applications should use the lowest privilege account needed to operate correctly.

Any logical communication ports should only communicate with specified services, with any services not required for device functions disabled. If a port is used for field diagnosis, then outputs should be disabled and provide no information that could potentially disclose credentials, memory addresses or function names.

The device should prevent null or empty passwords, disallow access to reference user accounts, have an incorrect login back-off mechanism, utilise secure cryptographic storage, and adhere to TS33.117 (3GPP, 2021) or NIST SP800-63B (Grassi et al., 2017). When inputting passwords, the input is to be obscured. The password reset mechanism should be assessed to ensure it cannot be abused. A secure timekeeping source that can be validated should be used as a source of system clocks. Devices should be able to recover to a known good state.

5.5.18.3.4.2 Weaknesses

No weaknesses where identified during comparison to the gold standard document.

5.5.18.3.4.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.18.3.4.4 Capability Summary

Table 96 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 96: IoTSF Secure Interface Management Summary

Strengths	Weaknesses	Other Observations
Secure Account Management	-	-
Principle of Least Access	-	-
Secure Time Source	-	-
Known Good State Recovery	-	-
Unique Identifiers	-	-
Restriction of Open Ports & Interfaces	-	-

5.5.18.3.5 Secure Update Mechanism

5.5.18.3.5.1 Strengths

Allow only authorized software to be installed, or if unauthorized software is to be run, it must run in a secure sandbox. The authorized software should be digitally signed, verified, and delivered over a secure encrypted channel. Once installed, authorized accounts can only perform downgrading of software. Updates should include the base operating system, which should be patched and up to date before release.

5.5.18.3.5.2 Weaknesses

No weaknesses were identified during comparison to the gold standard document.

5.5.18.3.5.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.18.3.5.4 Section Overview

Table 97 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 97: IoTSF Secure Update Mechanism Summary

Strengths	Weaknesses	Other Observations
Secure Update Channel	-	-
Unauthorized Software Sandbox	Sandboxing is not perfect and can be difficult	-
Downgrade Protections	-	-
Release State	-	-

5.5.18.3.6 Cybersecurity State Awareness

5.5.18.3.6.1 Strengths

An alert is to be raised when the device detects an attempted unauthorized change to its configuration.

5.5.18.3.6.2 Weaknesses

No weaknesses where identified during comparison to the gold standard document.

5.5.18.3.6.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.18.3.6.4 Section Overview

Table 98 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 98: IoTSF Cybersecurity State Awareness Summary

Strengths	Weaknesses	Other Observations
Malicious Activity Alerts	-	-

5.5.18.4 *Overall Summary Table: IoTSF*

Table 99 is a summary of all identified strengths, weaknesses and other notes gathered from the IoTSF document.

Table 99: IoTSF Overall Summary

Baseline Capability	Strengths	Weaknesses	Other Observations
Logical / Physical Identifiers	Manufacturer Hardware Identifier	Reliance on Manufacturer	-
	Unique Identifiers	-	-
Secure Interface Management	Firewall & Network Restrictions	Ambiguous 'Secure State'	-
	Up-To-Date Modern Cryptography	-	OWASP is not a conformance standard Import / Export Restrictions
	Secure Protocol & Communications	-	-
	Graceful Network Failures	-	-
	-	-	Device lifetime and support
Secure Software Configuration	-	-	Warning on device reset about security options
	Restoration to a Known Good State	-	-
	Secure Configuration	Ambiguous 'Sensitive Configuration Options'	Implicit audit logging
	Just-In-Time Provisioning	-	-
	Secure Password Storage	-	-
	Device Reset	-	-
	Secure Key Management & Provisioning	-	-
	Personal Data Management	-	-
Secure Interface Management	Secure Account Management	-	-
	Principle of Least Access	-	-
	Secure Time Source	-	-

	Known Good State Recovery	-	-
	Restriction of Open Ports & Interfaces	-	-
	Secure Update Channel	-	-
Secure Update Mechanism	Unauthorized Software Sandbox	Sandboxing is not perfect and can be difficult	-
	Downgrade Protections	-	-
	Release State		
	Malicious Activity Alerts	-	-
Cybersecurity State Awareness	-	-	-

5.5.19 Document Overview: OTA

The current document under analysis against the gold standard is Online Trust Alliance (OTA), (IoT Security & Privacy Trust Framework v2.5, 2017).

5.5.19.1 *Capability to Section Mappings*

Table 100 details the sections of each reviewed document as they relate to the NIST 'Security Capabilities' described in the "IoT Device Cybersecurity Capability Core Baseline". This document (IIC) is not prescribed in all capabilities, denoted by a '-'.

Table 100: OTA Document to NIST Document Mappings

Baseline Capability (NIST)	SECTION (OTA)
Logical / Physical Identifiers	-
Secure Software Configuration	26
Secure Data Storage & Transmission	2, 17, 33
Secure Interface Management	3, 12, 13 ,14, 15, 16
Secure Update Mechanism	1, 6, 8
Cybersecurity State Awareness	-

5.5.19.2 *Common Sections*

There are no common sections referenced in the NIST document.

5.5.19.3 *Capability Analysis*

The following section compares the guidance in the current document to the selected 'Gold Standard'.

5.5.19.3.1 Logical / Physical Identifiers

This section is not cross-referenced in the NIST document.

5.5.19.3.2 Secure Software Configuration

5.5.19.3.2.1 Strengths

An end-user must be able to review, edit and reset the privacy preferences of a device.

5.5.19.3.2.2 Weaknesses

No weaknesses were identified during comparison to the gold standard document.

5.5.19.3.2.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.19.3.2.4 Section Overview

Table 101 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 101: OTA Logical / Physical Identifiers Summary

Strengths	Weaknesses	Other Observations
Privacy Settings	-	-

5.5.19.3.3 Secure Data Storage & Transmission

5.5.19.3.3.1 Strengths

All personally identified information must be encrypted in both storage and transit. All Credentials should be salted, then hashed or encrypted and not stored in plain text.

5.5.19.3.3.2 Weaknesses

No weaknesses where identified during comparison to the gold standard document.

5.5.19.3.3.3 Other Observations

The statement that "devices and associated applications must support the generally accepted cryptographic practices" lack any additional guidance to aid in selecting the required functionality or tooling.

5.5.19.3.3.4 Section Overview

Table 102 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 102: OTA Secure Data Storage & Transmission Summary

Strengths	Weaknesses	Other Observations
Salt, Hash & Encrypt Credentials	-	-
-	-	Common cryptographic practices is a vague statement
Personal Information Encryption	-	-

5.5.19.3.4 Secure Interface Management

5.5.19.3.4.1 Strengths

All websites operating in support of IoT devices must always encrypt traffic in both directions of information flow. This should include technologies like HTTP Strict Transport Security (HSTS) and a reliable method to authenticate backend services and supporting applications. Devices should contain only the ports and connections required for functionality, with any unused ports disabled.

Strong authentication, such as single-use passwords or MFA, should be the default. Where needed, delineate between devices and services by requiring unique administrative passwords to service accounts.

Provide a generally accepted recovery process for users to regain access to accounts and passwords, including an out-of-band password change notification. Ensure that all accounts have a form of brute force protection.

5.5.19.3.4.2 Weaknesses

The respective impact of factory resets mentioned, though it is unclear if it refers to devices, support applications, administrative interfaces, or all four of these possibilities. Utilising individual administrative passwords for every device or system will require an organisation have established, mature processes, and a credential management system to be effective.

The phraseology ‘generally accepted’ or ‘commonly used’ is used without any additional guidance to aid in the implementation of what is being discussed.

5.5.19.3.4.3 Other Observations

Authentication of services and the required certificate management can be a large overhead if they follow best practices for individual certificates.

5.5.19.3.4.4 Section Overview

Table 103 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 103: OTA Secure Interface Management Summary

Strengths	Weaknesses	Other Observations
Bidirectional DLS/TLS	-	-
-	-	Certification management overhead Authentication of services is complicated
Minimal Functionality & Connectivity	-	-
Strong Authentication	Factory resets are vague and confusing	Unique passwords per device will require additional tooling
Account Recovery	-	-
Brute Force Protections	-	-
-	-	Vague phraseology without additional guidance

5.5.19.3.5 Secure Update Mechanism

5.5.19.3.5.1 Strengths

If the device can receive updates, the process must be disclosed, including timeframes, and required user actions. This update process may be automatic - if automatic, a rejection, limitation or deferral system must exist to allow finer-grained control of updates. These updates are to occur over a secure channel, and the code package should be digitally signed.

5.5.19.3.5.2 *Weaknesses*

The idea that a device may not be updatable is a reality where single-use IoT devices may exist (e.g., RFID Shipping Tags); however, this is not always acceptable for IoT device owners.

5.5.19.3.5.3 *Other Observations*

No other observations were made during comparison to the gold standard document.

5.5.19.3.5.4 *Section Overview*

Table 104 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 104: OTA Secure Update Mechanism Summary

Strengths	Weaknesses	Other Observations
Signed Updates	Devices may not be updateable	-

5.5.19.3.6 Cybersecurity State Awareness

This section is not cross-referenced in the NIST document.

5.5.19.4 *Overall Summary Table: OTA*

Table 105 is a summary of all identified strengths, weaknesses and other notes gathered from the OTA document.

Table 105: OTA Overall Summary

Baseline Capability	Strengths	Weaknesses	Other Observations
Secure Update Mechanism	Signed Updates	Devices may not be updateable	-
Secure Interface Management	Bidirectional DLS/TLS	-	-
	-	-	Certification management overhead Authentication of services is complicated
	Minimal Functionality & Connectivity	-	-
	Strong Authentication	Factory resets are vague and confusing	Unique passwords per device will require additional tooling
	Account Recovery	-	-

	Brute Force Protections	-	-
	-	-	Vague phraseology without additional guidance
Secure Data Storage and Transmission	Salt, Hash & Encrypt Credentials	-	-
	-	-	Common cryptographic practices is a vague statement
	Personal Information Encryption	-	-
Secure Software Configuration	Privacy Settings	-	-

5.5.20 Document Overview: NEMA

The current document under analysis against the gold standard is the National Electrical Manufacturers Association (NEMA), Cyber Hygiene Best Practises, (NEMA, 2018).

5.5.20.1 *Capability to Section Mappings*

Table 106 details each reviewed document's sections as they relate to the NIST 'Security Capabilities' described in the "IoT Device Cybersecurity Capability Core Baseline". This document (IIC) is not prescribed in all capabilities, denoted by a '-'.

Table 106: NEMA Document to NIST Document Mappings

Baseline Capability (NIST)	SECTION (NEMA)
Logical / Physical Identifiers	-
Secure Software Configuration	-
Secure Data Storage & Transmission	-
Secure Interface Management	Segmenting Networks, User Management, Hardening Devices
Secure Update Mechanism	Updating Devices
Cybersecurity State Awareness	Monitoring Devices and Systems

5.5.20.2 *Common Sections*

There are no common sections mentioned in more than one capability in the NIST document.

5.5.20.3 *Capability Analysis*

The following section compares the guidance in the current document to the selected 'Gold Standard'.

5.5.20.3.1 Logical / Physical Identifiers

This capability is not cross-referenced in the NIST document.

5.5.20.3.2 Secure Software Configuration

This capability is not cross-referenced in the NIST document.

5.5.20.3.3 Secure Data Storage & Transmission

This capability is not cross-referenced in the NIST document.

5.5.20.3.4 Secure Interface Management

5.5.20.3.4.1 Strengths

Ensure that an IoT network's design allows for logical segmentation and potential isolation of resources according to their purpose, with specific mentions of physical isolation of data conduits that need to transmit data between different network segments. There are multiple references used to supplement the information provided, with multiple references to the IEC 62443 Industrial Communication Networks (IEC 62443-4-2, 2019) document series. There are some examples of different zones and their potential additional security requirements provided. For wireless communications, the Service Set Identifiers (SSIDs) for higher security areas should be distinct from lower security areas. User management guidelines and responsibilities are delineated, with further extensive references to external documents. Some simple security issues to look out for and avoid are listed and explained.

5.5.20.3.4.2 Weaknesses

Data diodes may not be common vernacular outside of engineering fields.

5.5.20.3.4.3 Other Observations

The mentions of risk assessment and the multitude of ways that it can be performed does not provide implementation guidance on which way is acceptable in a given scenario.

5.5.20.3.4.4 Section Overview

Table 107 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 107: NEMA Secure Interface Management Summary

Strengths	Weaknesses	Other Observations
Secure Network Design	Uncommon Vernacular	-
Clear User Categories	-	-
Warnings of Simple Errors	-	-
Risk Assessment	-	No additional guidance for selecting risk assessment techniques

5.5.20.3.5 Secure Update Mechanism

5.5.20.3.5.1 Strengths

All IoT devices should be updatable based on any discovered vulnerabilities during their lifecycle. When a patch is not available, a manufacturer may issue countermeasures until a patch is available. A comprehensive risk assessment is bolstered by profuse external references to supplement the limited information provided around risk assessment.

5.5.20.3.5.2 Weaknesses

No weaknesses were identified during comparison to the gold standard document.

5.5.20.3.5.3 Other Observations

The guidance acknowledges that security needs will change across industry sectors. There is a single mention that not all devices are updatable, as their construction may preclude functionality. Bug bounty programs incur overhead that is not expanded on.

5.5.20.3.5.4 Section Overview

Table 108 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 108: NEMA Secure Update Mechanism Summary

Strengths	Weaknesses	Other Observations
Vulnerability Driven Updates	-	Needs shifting based on industry sector

Comprehensive Risk Assessment	-	-
-	-	Manufacturer bug-bounty programs
-	-	Non-Upgradable Devices

5.5.20.3.6 Cybersecurity State Awareness

5.5.20.3.6.1 Strengths

Well known and existing technologies are to be used to enable device monitoring, with an extensive list of external references. Specific usage of Simple Network Management Protocol Version 3 (SNMPv3) or above to take advantage of cybersecurity and feature enhancements. There is a discussion of what a SIEM captures and how it can aggregate other security devices into a single cohesive contextual information source.

5.5.20.3.6.2 Weaknesses

A comprehensive risk assessment is listed as required without additional guidance to perform or aid in selecting an approach.

5.5.20.3.6.3 Other Observations

The extraneousness statement of what a system log contains can be removed without detriment to the information provided.

5.5.20.3.6.3.1 Section Overview

Table 109 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 109: NEMA Cybersecurity State Awareness Summary

Well known & Existing Monitoring Technologies	No guidance for the comprehensive risk assessment	-
Use SNMP V3+	-	-
SIEM Usage	-	-
-	-	Extraneous system log explanation

5.5.20.4 *Document Overview*

Table 110 is a summary of all identified strengths, weaknesses and other notes gathered from the NEMA document.

Table 110: NEMA Overall Summary

Baseline Capability	Strengths	Weaknesses	Other Observations
Secure Interface Management	Secure Network Design	Uncommon Vernacular	-
	Clear User Categories	-	-
	Warnings of Simple Errors	-	-
	Risk Assessment	-	No additional guidance for selecting risk assessment techniques
Secure Update Mechanism	Vulnerability Driven Updates	-	Needs shifting based on industry sector
	Comprehensive Risk Assessment	-	
	-	-	Manufacturer bug-bounty programs
	-	-	Non-Upgradable Devices
Cybersecurity State Awareness	Well known & Existing Monitoring Technologies	No guidance for the comprehensive risk assessment	
	Use SNMP V3+	-	-
	SIEM Usage	-	-
	-	-	Extraneous system log explanation

5.5.21 Document Overview: OCF

The current document under analysis against the gold standard is the Open Connectivity Foundation (OCF), Security Specification (OCF Security Specification Version 2.1.2, 2020).

5.5.21.1 *Capability to Section Mappings*

Table 111 details each reviewed document's sections as they relate to the NIST 'Security Capabilities' described in the "IoT Device Cybersecurity Capability Core Baseline".

Table 111: OCF Document to NIST Document Mappings

Baseline Capability (NIST)	SECTION (OCF)
Logical / Physical Identifiers	7.1.1
Secure Software Configuration	5.3.3, 8.2, 12, 13.3.1
Secure Data Storage & Transmission	8.2, 11.2.1, 11.3, 14.2.2
Secure Interface Management	5.1, 5.2, 10
Secure Update Mechanism	14.5
Cybersecurity State Awareness	5.1, 5.7, 8.6, 12, 13.8, 13.16

5.5.21.2 *Common Sections*

5.5.21.2.1 OCF: Common Section: 5.1 - UUID

5.5.21.2.1.1 Strengths

The prescribed unique identifier type is a Universally Unique Identifier (UUID).

5.5.21.2.1.2 Weaknesses

No weaknesses were identified during comparison to the gold standard document.

5.5.21.2.1.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.21.2.2 OCF: Common Section: 8.2 –Device Reset

5.5.21.2.2.1 Strengths

A device can be reset to manufacturer defaults. This reset removes all data of both ownership and configuration.

5.5.21.2.2.2 Weaknesses

No weaknesses were identified during comparison to the gold standard document.

5.5.21.2.2.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.21.2.3 OCF: Common Section: 12: ACL Enforcement

5.5.21.2.3.1 Strengths

The server that controls a device enforces an Access Control List (ACL) over all actions a user or process takes.

5.5.21.2.3.2 *Weaknesses*

No weaknesses were identified during comparison to the gold standard document.

5.5.21.2.3.3 *Other Observations*

No other observations were made during comparison to the gold standard document.

5.5.21.2.4 Common Section Overview

Table 112 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 112: OCF Common Section Summary

Strengths	Weaknesses	Other Observations
Universally Unique Identifiers	-	-
Device Reset	-	-
ACL Enforcement	-	-

5.5.21.3 *Capability Analysis*

The following section compares the guidance in the current document to the selected 'Gold Standard'.

5.5.21.3.1 Logical / Physical Identifiers

5.5.21.3.1.1 *Strengths*

The prescribed unique identifier for all instances is a UUID.

5.5.21.3.1.2 *Weaknesses*

No weaknesses were identified during comparison to the gold standard document.

5.5.21.3.1.3 *Other Observations*

No other observations were made during comparison to the gold standard document.

5.5.21.3.1.4 *Section Overview*

Table 113 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 113: OCF Logical / Physical Identifiers Summary

Strengths	Weaknesses	Other Observations
Universally Unique Identifiers	-	-

5.5.21.3.2 Secure Software Configuration

See OCF: Common Section: 5.1 - UUID in addition.

5.5.21.3.2.1 Strengths

An Owner Transfer Method (OTM) must exist. The OTM is where the device is provisioned with secure credentials and registered in a management system. The secure credentials for a given device can be retrieved, updated, or deleted from a device.

5.5.21.3.2.2 Weaknesses

No weaknesses were identified during comparison to the gold standard document.

5.5.21.3.2.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.21.3.2.4 Section Overview

Table 114 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 114: OCF Secure Software Configuration Summary

Strengths	Weaknesses	Other Observations
Secure Provisioning	-	-
Credential Update	-	-

5.5.21.3.3 Secure Data Storage & Transmission

See OCF: Common Section: 8.2 –Device Reset in addition.

5.5.21.3.3.1 Strengths

Communications shall use a D/TLS version of at least 1.2, preferably the latest possible version. The supported cipher suites are listed in the Request for Comment series documents from the Internet Engineering Task Force, numbers 4279 (Tschofenig & Eronen, 2005), 4492 (Moeller et al., 2006), 5489 (Hajjeh & Badra, 2009) and 6655 (McGrew & Bailey, 2012).

A device is to use hardware-secure storage for symmetric or asymmetric private keys, certificate data, access credentials, or personal user information. Software emulated secure storage is not an acceptable alternative.

5.5.21.3.3.2 Weaknesses

No weaknesses were identified during comparison to the gold standard document.

5.5.21.3.3.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.21.3.3.4 Section Overview

Table 115 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 115: OCF Secure Data Storage & Transmission Summary

Strengths	Weaknesses	Other Observations
D/TLS Protocol Usage	-	-
Hardware Secure Storage	-	Software emulated secure storage is not acceptable

5.5.21.3.4 Secure Interface Management

See OCF: Common Section: 5.1 - UUID in addition.

5.5.21.3.4.1 Strengths

Device management servers should support the provisioning of Role Based Access Control (RBAC), Subject-Based Access Control (SBAC), and Wildcard Based Access Controls (WBAC). If using certificates for communication, the entire certificate chain is to be validated when establishing a connection. When accessing sensitive services, the server will authenticate the client, with the client able to assert roles.

5.5.21.3.4.2 Weaknesses

No weaknesses were identified during comparison to the gold standard document.

5.5.21.3.4.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.21.3.4.4 Section Overview

Table 116 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 116: OCF Secure Interface Management Summary

Strengths	Weaknesses	Other Observations
Multiple Access Control Schemas	-	-
Server-Side Authentication	-	-
Certificate Chain Validation	-	-

5.5.21.3.5 Secure Update Mechanism

5.5.21.3.5.1 Strengths

Manufacturers should have a clear policy outlining device updates and software vulnerabilities, including end of life and end of service updates and notices.

5.5.21.3.5.2 Weaknesses

No weaknesses were identified during comparison to the gold standard document.

5.5.21.3.5.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.21.3.5.4 Section Overview

Table 117 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 117: OCF Secure Update Mechanism Summary

Strengths	Weaknesses	Other Observations
Vulnerability Policy	-	-

5.5.21.3.6 Cybersecurity State Awareness

See OCF: Common Section: 5.1 - UUID and OCF: Common Section: 12: ACL Enforcement in addition.

5.5.21.3.6.1 Strengths

Auditable events logged by a device must be sortable by both a category and a priority. A device can be reset in a way that removes all configuration data but not the ownership information (a ‘soft’ reset). Provisioning should be possible from either a service push or client request. Endpoints shall be discoverable as specified by ISO/IEC 30118-1:2018 Information technology — Open

Connectivity Foundation (OCF) Specification — Part 1: Core specification (International Organization for Standardization / International Electrotechnical Commission, 2018).

5.5.21.3.6.2 Weaknesses

No weaknesses were identified during comparison to the gold standard document.

5.5.21.3.6.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.21.3.6.4 Section Overview

Table 118 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 118: OCF Cybersecurity State Awareness Summary

Strengths	Weaknesses	Other Observations
Auditable Events	-	-
Soft Device Reset	-	-
Endpoint Discoverable	-	-
Device Provisioning	-	-

5.5.21.4 *Document Overview*

Table 119 is a summary of all identified strengths, weaknesses and other notes gathered from the OCF document.

Table 119: OCF Overall Summary

Baseline Capability	Strengths	Weaknesses	Other Observations
Logical / Physical Identifiers	Universally Unique Identifiers	-	-
Secure Software Configuration	Secure Provisioning	-	-
	Credential Update	-	-
	ACL Enforcement	-	-
	Hard Device Reset	-	-
Secure Data Storage and Transmission	D/TLS Protocol Usage	-	-
	Hardware Secure Storage	-	Software emulated secure storage is not acceptable
Secure interface Management	Multiple Access Control Schemas	-	-
	Server-Side Authentication	-	-

	Certificate Chain Validation	-	-
Secure Update Mechanism	Vulnerability Policy	-	-
Cybersecurity State Awareness	Auditable Events	-	-
	“Soft” Device Reset	-	-
	Endpoint Discoverable	-	-
	Device Provisioning	-	-

5.5.22 Document Overview: PSA

The current document under analysis against the gold standard is the Platform Security Architecture (PSA), PSA Security Model (ARM Limited et al., 2020).

5.5.22.1 *Capability to Section Mappings*

Table 120 details each reviewed document's sections as they relate to the NIST ‘Security Capabilities’ described in the “IoT Device Cybersecurity Capability Core Baseline”.

Table 120: PSA Document to NIST Document Mappings

Baseline Capability (NIST)	SECTION (PSA)
Logical / Physical Identifiers	C1.4, R2.1
Secure Software Configuration	C2.3, R6.1, R7.1
Secure Data Storage & Transmission	C1.1, C1.4, C2.4, D5.2, R2.2, R2.3, R6.1, R7.1
Secure Interface Management	C2.3, D2.1, D2.2, D2.3, D2.4, D3.1, D3.3, R3.1, R3.2, R3.3, R4.2, R4.2, R6.1
Secure Update Mechanism	C2.1, C2.2, R1.1, R1.2, R6.1
Cybersecurity State Awareness	C1.3, D1.1, D3.2, D3.2, D3.5, D5.1, R4.1, R4.3, R4.4

5.5.22.2 *Common Sections*

5.5.22.2.1 PSA: Common Section: C1.4

5.5.22.2.1.1 Strengths

Device hardware will supply a Hardware Unique Key (HUK), with 128-bits of entropy, used for deriving other per device secrets. These secrets are - the Root of Trust Public Key (ROT-PK), used for authenticating the first stage of Secure Processing Environment (SPE) code during secure boot; a unique attestation key; an Instance ID that uniquely identifies the attestation key, and Implementation ID uniquely identifies the Immutable PSA-Root of Trust (PSA-RoT). These keys may be injected during manufacture by the device manager or generated by the devices when derived from a Physically Unique Function (PUF).

5.5.22.2.1.2 Weaknesses

No weaknesses were identified during comparison to the gold standard document.

5.5.22.2.1.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.22.2.2 PSA: Common Section: C2.3

5.5.22.2.2.1 Strengths

All software is to use the PSA-RoT provided Device ID for all Device ID related queries.

5.5.22.2.2.2 Weakness

No weaknesses were identified during comparison to the gold standard document.

5.5.22.2.2.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.22.2.3 PSA: Common Section: R6.1

5.5.22.2.3.1 Strengths

All changes to data residing in the PSA-RoT are to occur only after successful authentication.

5.5.22.2.3.2 Weakness

No weaknesses were identified during comparison to the gold standard document.

5.5.22.2.3.3 *Other Observations*

No other observations were made during comparison to the gold standard document.

5.5.22.2.4 Common Section Overview

Table 121 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 121: PSA Common Sections Summary

Strengths	Weaknesses	Other Observations
Secure Boot	-	-
Cryptographic Requirements	-	-
Secure Authentication	-	-

5.5.22.3 *Capability Analysis*

The following section compares the guidance in the current document to the selected 'Gold Standard'.

5.5.22.3.1 Logical / Physical Identifiers

See PSA: Common Section: C1.4 and PSA: Common Section: C2.34.

5.5.22.3.1.1 *Strengths*

No strengths were identified during comparison to the gold standard document.

5.5.22.3.1.2 *Weaknesses*

No other observations were made during comparison to the gold standard document.

5.5.22.3.1.3 *Other Observations*

No other observations were made during comparison to the gold standard document.

5.5.22.3.2 Secure Software Configuration

See PSA: Common Section: R6.1 in addition.

5.5.22.3.2.1 *Strengths*

The PSA-RoT is to act as the source of trust and the gatekeeper for all permitted modifications to data residing within the PSA-RoT.

5.5.22.3.2.2 *Weaknesses*

No weaknesses were identified during comparison to the gold standard document.

5.5.22.3.2.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.22.3.2.4 Section Overview

Table 122 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 122: PSA Secure Software Configuration Summary

Strengths	Weaknesses	Other Observations
Personal Data Management	-	-

5.5.22.3.3 Secure Data Storage & Transmission

See PSA: Common Section: C1.4 in addition.

5.5.22.3.3.1 Strengths

Hardware separation occurs between SPE and non-SPE areas of code execution. Cryptographic operations are to be in line with national security agencies' recommendations and at least 128 bits in strength, tailored to the nationality of deployment (e.g., Camelia may be used in Japan instead of ECDSA/AES). Hand-rolled, proprietary, or customised algorithms are not permitted.

Secure storage will contain all personal data. In addition, it is to store security keys and parameters and application data. If needed, these elements should be pinned to a device and its own known security state.

5.5.22.3.3.2 Weaknesses

No weaknesses were identified during comparison to the gold standard document.

5.5.22.3.3.3 Other Observations

Legacy applications may need to relax cryptography key sizes or algorithm specifications, but that must not negatively impact the overall cybersecurity schema.

5.5.22.3.3.4 Section Overview

Table 123 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 123: PSA Secure Data Storage & Transmission Summary

Strengths	Weaknesses	Other Observations
Hardware Secure Execution	-	-
Modern Cryptography	-	Legacy Provisions

5.5.22.3.4 Secure Interface Management

See PSA: Common Section: C1.4 and PSA: Common Section: R6.1 in addition.

5.5.22.3.4.1 Strengths

All unused network and logical interfaces are to be disabled. In addition, all debug or test features should be removed in production, with other unneeded functions or services disabled or uninstalled. When establishing communications, the device should be able to interrogate the server for authentication using secure and encrypted connections by default. These secure connections are to use a TLS version of at least 1.2 and forbid fallback to know insecure ciphers (e.g., 3DES, Null, DES, IDEA or RC4). Any security-related keys are to be encrypted at all times.

5.5.22.3.4.2 Weaknesses

Encryption is the default for stored secrets, but not mandated for all data.

5.5.22.3.4.3 Other Observations

Physical interfaces could be removed or locked, not just logically closed. Erasing a device on access to a debug interface presents a potential unwanted loss of data, and there is no mention of the potential impacts of deploying such a feature.

5.5.22.3.4.4 Section Overview

Table 124 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 124: PSA Secure Interface Management Summary

Strengths	Weaknesses	Other Observations
Removed Unused Ports	-	Physical Removal not mentioned
Encrypted Communications	Default, not mandated	Security-related data is always encrypted
Removal of Test/Debug Features	-	Erasure on access to these features is possibly contentious
Unneeded Services Removal	-	-

5.5.22.3.5 Secure Update Mechanism

See PSA: Common Section: R6.1 in addition.

5.5.22.3.5.1 Strengths

The PSA-RoT can perform firmware updates (to itself) either by remote push, or locally. These updates must be checked to ascertain the validity, file content, and overall package state via a secure cryptographic means in line with the requirements (128-Bits, no vulnerable ciphers, no proprietary ciphers, no modifications, and adherers to NSA FIPS Guidelines). This update mechanism must in incorporate a form of anti-rollback protection, either via read-only storage or MFA codes.

5.5.22.3.5.2 Weaknesses

No weaknesses were identified during comparison to the gold standard document.

5.5.22.3.5.3 Other Observations

No other observations were made during comparison to the gold standard document.

5.5.22.3.5.4 Section Overview

Table 125 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 125: PSA Secure Update Mechanism Summary

Strengths	Weaknesses	Other Observations
Secure Firmware Updates	-	-

5.5.22.3.6 Cybersecurity State Awareness

5.5.22.3.6.1 Strengths

The device is to support acknowledgement of its current and set state. At a minimum, it must support the following: Assembly, Test, Factory Provision, Provisioned, and Debug. The device must use a Secure Boot mechanism that is backed by the PSA-RoT. Logfile access is restricted to authorized users only.

5.5.22.3.6.2 *Weaknesses*

State transitions are listed as optional in some areas, which is detrimental when the state transitions are implied to be mandatory. Logging of events is also listed as optional function.

5.5.22.3.6.3 *Other Observations*

If secure states are implemented, then the device must support the interrogation of its current state. The capability for logging is duplicated, describing different levels of access and privacy, seemingly to prevent personal data access that might have been caught in log files being exposed.

5.5.22.3.6.4 *Section Overview*

Table 126 is a summary of the identified strengths, weaknesses, and other notes identified during the capability analysis.

Table 126: PSA Cybersecurity State Awareness Summary

Strengths	Weaknesses	Other Observations
State Awareness & Transitions	Currently Optional	Interrogation of current cybersecurity state
Secure Boot	-	-
Restricted Log Access	Logging is optional	Duplication of restriction to authorized users under a different section

5.5.22.4 *Overall Summary Table: PSA*

Table 127 is a summary of all identified strengths, weaknesses and other notes gathered from the PSA document.

Table 127: PSA Overall Summary

Baseline Capability	Strengths	Weaknesses	Other Observations
Secure Software Configuration	Secure Boot	-	-
Secure Data Storage and Transmission	Cryptographic Requirements	-	-
	Personal Data Management	-	-
	Modern Cryptography	-	Legacy Provisions
	Encrypted Communications	Default, not mandated	Security related data is always encrypted

Secure Interface Management	Secure Authentication	-	-
	Removed Unused Ports	-	Physical Removal not mentioned
	Removal of Test/Debug Features	-	Erasure on access to these features is possibly contentious
	Unneeded Services Removal	-	-
Secure Software Configuration	Hardware Secure Execution	-	-
Secure Update Mechanism	Secure Firmware Updates	-	-
Cybersecurity State Awareness	State Awareness & Transitions	Currently Optional	Interrogation of Current State
	Restricted Log Access	Logging is Optional	Duplication of restriction to authorized users under a different section

5.6 CONCLUSIONS

The differences in the target audiences, level of technical detail, and view of the IoT ecosystem were assumed to exist when starting the data gathering, although not to the level that was discovered. The analyses uncovered a lack of systematic approach to cybersecurity, with only technical specifications (OCF, PSA) providing a technical basis for cybersecurity. The other documents (AGELIGHT, BITAG, CSA, CSDE, CTIA, ENIMA, ETSO, GSMA, IEC, IIC, IoTSF, OTA, and NEMA) varied greatly in the level of technical guidance presented, with an overall dependence upon the capabilities of an individual IoT device to provide the requisite functionality for security operations. These capabilities are fragmented due to the disconnected goals of the documents.

5.6.1 Overall Insights

Overall, the analysed documents agreed on the actions to apply effective cybersecurity to IoT devices and IoT networks at a conceptual level. However, a conceptual level agreement is not constructive when it comes to implementation, particularly given the diverse and disparate nature of IoT devices and their associated ecosystems. When technical details are missing, the onus of what technical controls to implement shifts to the implementer, who is not guaranteed to have the required knowledge. This lack of knowledge is compounded by the myriad of possibilities when implanting a given technical control. In line with contemporary best practice, the gold standard of cybersecurity should be presented in technical detail, allowing implementers to explicitly relax security requirements, which is the 'secure by default' approach.

5.6.2 Characteristic Summary

Figure 30 presents the common strengths of all analysed documents. The common actions were further deconstructed into the degree of presence with the documents, that is, the overall guidance's effectiveness. This deconstruction was obtained by the synthesis of identified, strengths, weakness, and other observations during the document analysis in comparison to the perceived gold standard. The 'extracted capabilities' are the synthesis of common actions or requirements that were noted during the document analysis.

	Document														
Extracted Capability	AGELIGHT	BITAG	CSA	CSDE	CTIA	ENISA	ETSI	GSMA	IEC	IIC	IoTSF	OTA	NEMA	OCF	PSA
Use Modern Cryptography	●	●	◍	●	◍	●	◍	◍	◍	●	●	◍	◍	◍	●
Secure Data Storage	●	○	◍	◍	○	◍	○	◍	●	◍	●	●	○	○	◍
Cybersecurity Policies	●	◍	◍	◍	◍	◍	◍	◍	◍	●	◍	◍	◍	●	◍
Device Reset / Refresh	●	◍	◍	◍	◍	◍	◍	◍	◍	◍	●	◍	◍	●	●
Endpoint Management	●	●	◍	○	○	●	●	●	●	○	●	◍	◍	◍	●
Strong or No Defaults	●	●	●	○	○	●	○	○	○	○	●	○	◍	◍	○
Secure Provisioning and Updates	●	●	●	●	●	●	●	●	●	●	●	●	◍	●	●
No Deprecated / Vulnerable Protocols	○	●	◍	●	●	●	○	●	●	◍	●	●	○	●	●
Testing and Security Hardening	◍	●	○	○	●	○	○	○	○	○	○	○	◍	○	○
Event Logging and Auditing	○	○	○	●	●	●	●	●	●	●	○	○	●	●	◍
Hardware Secure Computation	○	○	○	●	○	●	●	●	◍	◍	○	○	○	●	●
Hardware Secure Storage	○	○	○	●	○	●	●	●	◍	◍	○	○	○	●	●
Authentication and Authorisation	○	○	●	◍	◍	◍	○	●	●	◍	◍	●	◍	◍	●
Organisational Maturity	●	●	●	◍	○	◍	◍	●	◍	●	◍	○	○	○	◍

Figure 30: Document Characteristic Strengths Matrix (Black = Strong, Grey = Average, White = Weak)

5.6.2.1 *Use Modern Cryptography*

Use Modern Cryptography is defined as:

Strong:

- The use of modern, tested, verifiable and peer-reviewed cryptographic implementations and algorithms
- This usually coincides with reference to either the FIPS (National Institute of Standards and Technology, 2019) or other NIST based documents handling cryptography

- A good addition is the reminder to not ‘hand-roll’ or implements proprietary cryptography, although it is not always stated explicitly

Average:

- The actions provide some explanation and guidance on why cryptography is essential and the requirements of implementing cryptography
- Some mention of protocols or external references

Weak:

- Cryptography is either implied by other functions or has a brief mention with no additional guidance or external references

5.6.2.2 *Secure Data Storage*

Secure Data Storage is defined as:

Strong:

- The handling of data and credentials at all stages (creation, movement, storage, deletion) is prescribed
- Authentication utilises known and tested authentication protocols and ensures the passwords are stored securely (salted, hashed or encrypted, preferably all three) via non-compromised algorithms
- Data storage is by hardware-backed dedicated storage, with direct mention of hardware-level encryption

Average:

- Credentials are prescribed as not in plain text and encrypted, without specific requirements provided for algorithm selection or storage
- There is an explanation of the importance and potential issues to avoid.
- Minor external references

Weak:

- Credential management is prescribed as ‘secure’
- There is little or no additional guidance provided or reference to additional information

5.6.2.3 *Cybersecurity Policies*

Cybersecurity Policies is defined as:

Strong:

- Implement policies governing the actions prescribed or adding existing policies to cater to IoT and its associated challenges specifically
- Specific goals or desirable outcomes are given to outline policies

- Given the internal nature of polices, it is very much 'left to the implementer' as there is no templated approach to internal policy creation or modification that is universally applicable

Average:

- Some policies are presented with an outline of what these policies would need to contain, and their end-goals are provided
- There is little external guidance
- It is implied that existing policies should form the basis of the new policies

Weak:

- Policies are not mentioned or are implied by other prescribed actions
- Little or no external guidance is provided

5.6.2.4 *Device Reset and Refresh*

Device Reset and Refresh is defined as:

Strong:

- The ability to reset a device to factory defaults, wiping all data from the device as well as any associated cloud or backend services
  - This 'hard reset' is analogous to a 'factory reset'
- The ability to refresh a device, reverting it to default system settings, and keeping most user-level configurations and data
- Specific mentions of regulatory adherence and requirements

Average:

- Either device reset or device refresh is mentioned, but not both
- Brief mentions of regulatory adherence and connected systems
- Some external guidance

Weak:

- The action is not mentioned or implied by other actions
- No mention of eternal guidance, regulatory concerns or connected systems data

5.6.2.5 *Endpoint Management*

Endpoint Management is defined as:

Strong:

- The management of all connection endpoints is specifically called for

- This includes removing unused logical and physical connections, monitoring, authentication, authorization, removing debug or serial ports, segregation of managerial traffic, and the usage of encryption
- Any external guidance mentioned here is usually for specific aspects that require more detail – e.g., authentication or encryption

Average:

- Some protections are mentioned, usually deactivation of unused ports and debug interfaces, with some authentication and authorization methods prescribed

Weak:

- Endpoints are implied to be the primary security focus of other capacities or mentioned briefly with minimal explanation or expansion

5.6.2.6 *Strong or No Defaults*

Strong or No Defaults is defined as:

Strong:

- If default settings exist, ensure that they do not degrade the security of a device
- This is sometimes prescribed as disallowing defaults, requiring that they be changed during the provisioning process

Average:

- Defaults are described or mentioned as needed to be secure, but few or no specific actions are mandated

Weak:

- Defaults are not mentioned or implied by other aspects

5.6.2.7 *Secure Provisioning and Updates*

Secure Provisioning and Updates is defined as:

Strong:

- An update and provisioning method that considers over-the-air and over-the-wire updates, cryptographic update verification, downgrade protections and trusted update sources

Average:

- Updates are described as secure, with some protections supplied, but missing aspects - e.g., a secure update source, but no mention of code verification of the device's update files

Weak:

- The actions taken are prescribed as secure, but no specific guidance is provided.

5.6.2.8 *No Deprecated or Vulnerable Protocols*

No Deprecated or Vulnerable Protocols is defined as:

Strong:

- Utilise the latest possible versions of protocols that do not have a known vulnerability

Average:

- A protocol is mentioned but either not prescribed as a mandatory action nor explicitly stated to use both the latest version and a version with no known vulnerabilities

Weak:

- No specific protocols are prescribed, or if they are, they are mentioned by name without any further explanation or requirement

5.6.2.9 *Testing and Security Hardening*

Testing and Security Hardening is defined as:

Strong:

- Having both a testing plan to verify security measures and performing security-hardened based on these tests' results
- Ongoing testing

Average:

- A testing plan is mentioned but not expanded on as to its aims, goals, or function

Weak:

- There is no mention of a testing plan for a security hardening process

5.6.2.10 *Event Logging and Auditing*

Event Logging and Auditing is defined as:

Strong:

- Having devices store and report events in sufficient detail that analysis and auditing can occur in both real-time and post-incident
- This usually involved both on-device storage and centrally storage, along with integration into a SIEM
- There are specific mentions of log access restrictions
- Specific events or event categories are provided

Average:

- Mentions of an audit log and its intended usage
- Some mention or event type or categories, with mention of central storage of SIEM integration

Weak:

- Brief or implied mentions of logging without further details

5.6.2.11 *Hardware Secure Storage and Computation*

Hardware Secure Storage and Computation is defined as:

Strong:

- Encrypted storage on the device that is implemented via hardware, requiring a dedicated API to facilitate data retrieval or storage
- Guidance on what data is to be stored in the hardware-secure storage

Average:

- Mention of hardware secure storage or other encrypted storage, with specific mention of what should be stored or the storage requirements

Weak:

- No mention of hardware back secure storage or other secure storage

5.6.2.12 *Authentication and Authorization*

Authentication and Authorization is defined as:

Strong:

- Both authentication and authorization are mentioned in detail, with a clear delineation of responsibilities

- Clear advice to use known, verified and tested protocols, with provisions for devices that may not support them
- Supplementary external references are present

Average:

- Authentication and authorization are mentioned but not explicitly explained
- Some modern protocols are mentioned by name, without additional information
- Some supplemental guidance

Weak:

- Authentication or authorization are implied by functionality and not explicitly stated or conflated together and presented in an unclear manner
- No or outdated supplemental guidance

5.6.2.13 *Organisation Maturity*

Organisation Maturity is defined as:

Strong:

- The organisation's requirements to undertake the prescribed actions are highly detailed, with clear actions prescribed to roles

Average:

- Some requirements are listed and may be assigned to roles

Weak:

- All aspects of organisational maturity are implied as existing
- The assumed level of organisation maturity to handle complex, multifaceted tasks in a defined and reproducible manner is relatively high, relying on expertise (internal or external) to facilitate and drive these changes

5.6.3 Additional Findings

The following section expand on the common concepts, notes and additional points of interest that were discovered during the analysis.

5.6.3.1 *Common Concepts*

A ‘common concept’ is a concept about the application of IoT cybersecurity that was recurring across documents during the analysis.

5.6.3.1.1 Hardware-Based Secure Storage and Root of Trust

The Root of Trust is a well-understood concept that applies across all computing areas to aid in the application of cybersecurity. Modern hardware usually contains some form of Trusted Computing Module (TCM) or Trusted Platform Module (TPM) – specialised hardware dedicated to verification of specific segments of code, providing a secure environment for storing secret information, generating cryptographic keys, and implementing cryptographic functions such as encryption and digital signatures (Gallery & Mitchell, 2009).

Many of the secure functions specified by the documents analysed (storage, reporting, verification, or updating of software and data) depend on hardware level support. Without this hardware support, the Root of Trust is far more difficult to establish, however hardware support in IoT devices is not guaranteed. Hardware support for trusted computing in IoT can include issues such as the reliance on manufacturers to ensure that across all IoT devices manufactured, when performing customisations, identifiers are not duplicated, with the trusted computing module also forming a segment of supply chain management and the secure hardware functionality. Who is responsible for what identifier and system can be contentious, with the scale of devices acting as an additional challenge to addressing these issues.

A common approach is to utilise X.509 Cryptographic Certificates (Boeyen et al., 2008) to control trust boundaries and establish communications. Overall, several areas can depend on the Root of Trust setup, leads to a realisation of a ‘Single Point of Failure’. These potential failures can include in a sectional hierarchy, the loss of a higher key exposes all devices below the compromise, certificate renewal can take extensive amounts of time, and is not always automatable, databases of stored credentials are vulnerable to cyber-attacks, heavy cryptographic processing is not always possible on an IoT device and that the IoT hardware supports all the functions required.

More recently, however, the definition of what constitutes ‘Trusted Computing Functionality’ has been revised and extended to incorporate the concepts of a secure boot process (Gallery & Mitchell, 2009). This enables a platform's state to be reliably measured, verified, and recorded; and software isolation, which supports the unhindered execution of software, safe from interference by other software running on the same platform. The application of these concepts to the resource constrained IoT ecosystem presents its own unique set of challenges.

5.6.3.1.2 End Points

IoT standards have moved away from analysing the device, towards analysing the multiple communication endpoints on a device. The description of an endpoint is described as 'a point of communication', abstracting away the mechanism when possible. This marks a change from the traditional cybersecurity perspective of treating a device as a standalone aspect, securing the device itself, with communications coming as a secondary part of the device. This approach of endpoint security is not new, as many enterprise cybersecurity solutions purport themselves as 'endpoint security'.

This conceptual shift to a focus on communications as opposed to the devices can be attributed to the capabilities of the devices. IoT devices can vary significantly in capabilities between individual IoT devices and are also radically different from traditional computing devices (phones, laptops, desktops, servers). These large differences create an IoT ecosystem where generic programs that can consume significant resources to deal with a wide variety of devices and situations are not always feasible for deployment or use.

5.6.3.1.3 Unique Identification

All documents agreed that devices need to be able to be identified uniquely. The methods described (or lack thereof) disagree on what constitutes a 'strong' identifier. Some, like the PSA, mandated a Universally Unique Identifier (UUID) injected into a devices secure processing mechanism at time of manufacture as its identification – others allowed for any logical identifier to be used, like a MAC address. Given that some logical identifiers can be spoofed in a trivial manner, they may not be suitable for usage as an identifier for cybersecurity purposes.

5.6.3.1.4 Hardware Level Security

Many prescribed cryptographic operations rely on hardware level support, with some explicit mention that software alternatives are not acceptable for some functions. Dedicated secure storage and computational systems that are physically segregated allow for a higher degree of separation of data and processing. This will depend highly on the device itself, the software, and the Application Programming Interface (API) to enable this.

5.6.3.1.5 Security by Design

Security should be a part of all considerations at initiation and not enabled by patches or later updates. This creates a need for specialised security knowledge integrated into all aspects of a device – from initial concept and design, through installation and use, to decommissioning and disposal.

5.6.3.2 *General Observations*

The following observations are applicable across the analysed guidance addressing miscellaneous issues or omissions that were identified during analysis. The term miscellaneous should not be construed as afterthoughts, as these observations still identify significant areas where issues could arise.

5.6.3.2.1 Generic Guidance

Excluding the industry-specific documents (GSMA, IIC), or technical specifications (PSA, OCF), the provided guidance and capabilities are broad and generic. This leaves the implementation of this guidance reliant on external guidance (if provided) or internal knowledge. As such, the genericness of most documents is a detriment to the effective application of the principles discussed within the documents.

5.6.3.2.2 Best Practice

Often, the guidance refers to best practice. While this makes sense to professionals in the field, best practice is an ever-shifting target and significantly bound to the current knowledge of an area. Thus, should somebody not have the current, latest knowledge of best practice, the subsequent inadequate guidance presented represents a significant potential for poor implementation of cybersecurity technical controls.

5.6.3.2.3 Specialised, Disparate Target Audiences

As briefly highlighted in 5.4.4 Common Audiences, there is great variation in intended audience. This variation in the target audience also creates a difference in the discussion points – managers are not as concerned with technical details and specifics as an engineer is. This creates an imbalance of guidance where, given that the guidance analysed is skewed towards higher-level principles instead of technical specifications, the presented information is lacking the technical details to implement the designated principles.

5.6.3.2.4 Device Management

Centralised device management is an ongoing issue and can still be performed badly for traditional computing devices. Mobile Device Management (MDM) and its subset, Bring-Your-Own-Device (BYOD) are still potential pain points for cybersecurity. These pain points are compounded by requiring the reinvention of large segments of the current MDM approach, as much of the IoT ecosystem will not be monitorable or integrate with existing platforms and software. The majority of the analysed documents assume a gamut of abilities present in IoT devices, IoT device management software and hardware and the ability to integrate to existing software stacks. The process of MDM was rarely mentioned in detail, and instead was inferred by requirements of other actions.

5.6.3.2.5 Hardware Support

The overall view is that IoT cybersecurity must be present from device inception, vertically integrated at all levels, and not an isolated layer or action. This requires stringent manufacturing and software capabilities that will not be present on all IoT devices. While the goals are admirable, they are almost universally dependent on hardware-enabled cryptography that will not be present in all devices. Some guidance specified identifiers are be injected into firmware at time of manufacture – which, again, is not guaranteed as an IoT chip is almost certain to be an amalgamation of multiple controllers, sensors, and computing packages.

5.6.3.3 *Tangential Security*

All documents had tangential mentions of other established areas of security in varying levels of detail. Some aspects were mentioned as important but bereft of additional guidance (e.g., physical security and device management). Others are implied by some capability or mentioned briefly in an incidental manner. These secondary mentions included supply chain security and device management.

5.6.3.3.1 Complicated Capability Overlap

Cybersecurity is an interrelated discipline, with very few aspects existing in a stand-alone manner. This interconnection represents a difficulty in explaining and representing all of cybersecurity. Take, for example, cryptography; used in data storage, transmission, memory management and hardware - nearly every area of computing. Each unique area utilises a basic set of cryptographic functions, with the exact function varying broadly, based on contextual inferences – each requiring its own detailed analysis and explanations.

5.6.3.3.2 Varying Level of Detail

The guidance provided runs the gamut of detailed explanations, even within the same document. Some aspects of security are clearly defined, delineated, and explained. A paraphrased example of such is - all communications should use at least D/TLS 1.2, preferably the latest available version, or equivalent publicly verified protocol that contains no (publicly) known vulnerabilities, with at least 128-bit AES key strength or equivalent, higher if possible. This level of guidance is comprehensive – it provides a clear baseline and tangible requirements that can be implemented by any level of technical professional without any ambiguity in implementation. At the other end some documents have broad, sweeping, generic guidelines; for example – *a unique value for each endpoint must exist to allow for a device or endpoint to be distinguished from all other endpoints*. While there may be some discussion around why this is important, not all identifiers (particularly logical identifiers) are non-fungible. The overall lack of contextual guidance is of import here, as what constitutes an acceptable identifier will be radically different for differing security contexts.

5.7 Issues Encountered During Case

This case presented multiple significant issues that radically changed the overall research goals. The analysis of the selected documents was initially envisioned as a formal checklist – that the existing body of knowledge for cybersecurity on traditional devices would have mostly made the transition across to IoT, with sufficient technical detail to allow a professional in the field to make corrections for any ecosystem differences. Instead, there was a segmented, fit for purpose, and presumptive scattering of standards, ranging widely in details and perspective.

These different outlooks ranged from a generic principal level overview to a technical testing and certification standard – this is demonstrated through a lack of systems or process-based standards. These systems-based standards were occasionally referenced (e.g., ISO 27001 (ISO/IEC, 2013), but not universally. This reflected the fragmentation of cybersecurity controls across documents, and this fragmentation was the cause of the major shift in the research outlook.

5.8 CHANGES TO RESEARCHERS' VIEWS

This research assumed that the existing body of knowledge would be used, referenced, and technically adapted to suit the new challenges in the IoT ecosystem in detail. The analysis shows that dependence on this knowledge was implicit in most cases, assumed in others and rarely stated; that a body of proven knowledge exists is no guarantee that it will be used, despite the obvious and tangible benefits of doing so.

Due to the disparate perspectives and controls presented, the research shifted drastically from a cataloguing the presented guidance to a thorough, in-depth analysis of the presented guidance to address the identified issues. To remediate this, the subsequent cases (Case 3 & Case 4) were removed from the research, as the issues would propagate through any additional cases. This is due to both the structure of the research and the nature of cybersecurity. For the structure of the research, each sub-case aims to gather information on a specific aspect within the overall case. This sub-case analysis allows for the dynamic pivoting and retargeting of the research overall, as each sub-case, while contained with an overall scope defined by its outer case, is its own self-contained case study.

As such, the finding from Case 2-A, which would nominally feed into an eventual cross analysis as defined in Section 3.3.7 with all other cases (Cases 2-B,C,D,E,F, Case 4-A,B,C and Case 5-A,B,C), it is this feed-in of information that creates the issue and the reason for discarding subsequently planned cases. If the subsequent cases were tied directly to the initial case via this feed-in of data during the cross analysis, the issues identified in Case 2-A would create a knowingly deficient baseline, creating the dilemma of basing cybersecurity protections off knowingly flawed protections – which would directly affect the ability of this research to answer the questions posed. As cybersecurity protections must work within a system of systems, the very nature of cybersecurity also precluded continuing with additional cases, as again, a knowingly flawed basis should not be used to derive cybersecurity protections.

Finally, these issues presented a significant issue in presentation of data. Presenting so many different viewpoints in a manner that is clear, cohesive, and understandable took over a dozen major revisions and changes to the presentation of the entire document.

5.9 LEARNING FROM CASE

This case (Case 2-A) applied the learning from the first case (Case 1), that is, that data presentation must be more flexible and may not always be words. As such, the main data delivery of this case is diagrams and tables, supported by words. To use a trite analogy, the case presentation is more akin to Jenga blocks, where each piece is useful on its own, but are stacked carefully to construct the overall view of the case. This approach of segmented analysis is an important learning from this case – the ability to break an argument into smaller chunks for clarity and understanding, without compromising the overall argument. To better articulate the overall personal learning from this case (Case 2-A), the approach of 'levels of learning' as described by Checkland (1991) is used. The usage a level system aid in understanding and articulating, as "The creation of information from data is a uniquely human act" (Checkland, 1991).

A 'Level 1' learning is described as "what has been learnt from this piece of research and the research themes?" (Williams, 2007). A 'Level 2' learning is described as "what does this research contribute to the overall research project? Is it consistent with the research objectives?" (Williams, 2007). Each of these levels answered (as related to Case 2-A) in the following sections.

5.9.1 Level 1 learning

The area of investigation has far more issues than initially estimated. The guidance provided is extensive, but it not technical enough to give solid guidance for implementers. It is instead heavily focussed on managerial and general principles, leaving technical choices and implementation up to professional or organisation knowledge that cannot be depended on to be consistent or up to date with current technical means.

5.9.2 Level 2 learning

The identification of the current lack of a detail and specific standard that deals directly with IoT security that is not tied to an industry body or device certification program. Such a document should address IoT in a generic manner but provide technical baseline details that should define a minimum acceptable level of security. Above all, it should be unambiguous and implementable by a professional that may not have direct industry knowledge of cybersecurity.

6 ANALYSIS

The analysis of the identified IoT characteristics against the selected 'Trusted Industry Benchmark' (TIB) (National Institute of Standards and Technology, 2018) (Section 5.5.2) allows for a comparison of issues that affect the broader IoT ecosystem and the technical specifications required for cybersecurity. By using a trusted and mature base, the analysis highlights where the IoT cybersecurity guidance is not yet as mature as the existing body of knowledge for traditional computing and therefore, leads to incomplete protection. This multi-level analysis is the basis for the answer to the primary research question of 'How do we create a framework for IoT Cybersecurity?'.

This analysis requires two stages – a high level, ecosystem-wide identification of issues and concepts that are lacking when compared against contemporary cybersecurity practices (Section 4, Case 1), and a subsequent detailed technical analysis. The IoT ecosystem level issues alter the selection of approaches and solutions to the applications of cybersecurity – they also can define the limitations of IoT that will need addressing – as well as identify if the limitation originates from the IoT devices, processes surrounding IoT, ecosystem or other sources.

The second stage detailed technical analysis compares the guidance extracted from the selected documents (Section 5, Case 2-A) to the TIB, highlighting the differences in coverage and approaches. This technical 'low-level' analysis is needed to capture and account for the technological differences associated with IoT. To perform this analysis, there are two stages of comparison, mirroring the TIB. Firstly, an overall comparison against the *Function* as identified by the TIB. A *Function* organises cybersecurity actions into broad principles. As an example, the *Identify function* is defined as "Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities." (National Institute of Standards and Technology, 2018, p. 7). The mapping of *Functions* to *IoT Capabilities* is shown in Table 128.

Table 128: NIST Function to IoT Capability

NIST Function	NIST IoT Capability
Identify	Logical / Physical Identifiers
Protect	Secure Software Configuration, Secure Data Storage / Transmission, Secure Interface Management, Secure Update Mechanism
Detect	State Awareness

Respond	Not Present
Recover	Not Present

Secondly, the analysis of the actions required by each *function* is undertaken. This secondary stage is concerned with both *Categories* and *Sub-Categories*. A *Category* is a sub-division of a function into a logical group – examples of *Categories* are Asset Management, Response Planning, or Detection Processes. A *Sub-Category* divides a *Category* into a set of technical or management activities that have a clear outcome – examples of *Sub-Categories* are Incident Containment, Update Strategies, or Roles and Responsibilities. An example of this mapping is shown in Table 129.

Table 129: Identity Function Categories to IoT Capability

Identity Function Categories	IoT Capability
Asset Management	Logical / Physical Identification
Business Environment	Not Present
Governance	Not Present
Risk Assessment	Not Present
Risk Management Strategy	Not Present
Supply Chain Risk Management	Not Present

The comparison of the ecosystem followed by a deeper technical analysis will provide different levels of information on how the existing IoT guidance compares to the TIB and the existing body of cybersecurity knowledge (EBoK). It will allow for the identification of:

- Where the TIB and EBoK can be translated to IoT without issue,
- Areas where the IoT guidance is at a similar level of maturity as the TIB and EBoK,
- Areas of omission in the IoT guidance, and
- Areas of weakness in the IoT guidance

With the known areas of omission, weakness, comparative strength and possible translations, this information has been used to create a framework for the application of cybersecurity to IoT. By using the TIB as a basis, the new framework created from this research functions best as an overlay to existing guidance, highlighting the areas where additional effort is needed to modify cybersecurity approaches to IoT.

6.1 Ecosystem Wide IoT Attributes

The ecosystem of IoT contains unique characteristics that shape the application of cybersecurity for all IoT devices. These characteristics range from technical limitations of IoT devices to the management and process alterations required to account for IoT. As these common issues are tied to the ecosystem of IoT, they should be included in any detailed discussion. These are discussed in the same order as they appear in Figure 30.

6.1.1 Cyber-Physical Systems (CPS)

Cyber-physical systems (CPS) can be described as a system with both a digital presence that has control over physical object(s) or affects. These systems range from large scale actions like opening sluice gates on a dam to smaller actions, like unlocking doors. This application of IoT is a relative of the existing SCADA networks (Section 2.2), which are usually industrially focused and use dedicated hardware to control physical actions. While not wholly accurate to call CPS the next evolution of SCADA, it is accurate enough to illustrate the potential issues that can occur when connecting digital devices to 'real world' actions. This link of digital command to tangible actions is further complicated by the multitude of different actions a single IoT device can perform. Existing SCADA equipment is also multi action; however, SCADA networks are generally dedicated hardware that is not as flexible, integrated or connected as IoT devices. This means that risk of a device compromise must also include the potentially multiple downstream physical actions that could also occur.

6.1.2 Organisational Maturity

The size and maturity of an organisation will shape the approach to IoT and cybersecurity in general. Smaller organisations are often resource-constrained but able to more rapidly adopt and discard approaches to IoT or technologies. In comparison, more significant organisations are less agile but able to apply more resources to an activity. This difference in resource application results in the larger organisations reaching the issue of IoT Scaling and IoT Device Management sooner than smaller organisations.

6.1.3 Modern Cryptography

The application of modern cryptography touches almost every facet of a daily life – the reliance on keeping what must be secret, secret, demonstrates how critical it is to ensure that cryptographic operations function as expected. The application of this principle is universal – it makes no different if the secret information is from IoT devices, a datacentre, a mobile phone or even written on paper.

In most cases, the guidance to use modern cryptography is enough for a professional to, with minimal to no additional research, ascertain the requirements of a given deployment. It is where this additional research moves beyond trivial that a severe potential gap occurs. This gap that can range from mild and inconsequential to catastrophic and is highly dependent on the professionals' contextual forces; time, effort, knowledge, and skill are just a few that can impact how the selection and implementation of secure protocols.

This can be addressed by filling the gap in the guidance – explicitly naming the protocols, settings, and suites where possible, linking to clear and direct additional information like the NIST FIPS guidance when this is not feasible. It is impossible to control the context around what data is essential for that specific instance – the guidance should present the gold standard, then clearly show the areas that can be lessened or changes to different restrictions without compromising other tangential functions that depend on a secure cryptographic base. Finally, cryptographic algorithms can potentially fall under regulatory oversight, the usage and associated overhead of cryptographic operations on IoT devices may be restricted by their operational location.

6.1.4 Secure Data Storage and Transmission

Secure Data Storage and Transmission (SDST) is comprised of two distinct yet interrelated processes for handling digital data – Data Storage and Data Transmission. These two processes are intrinsically linked and are best discussed together. Both discrete processes rely heavily on cryptographic operations to provide the secure aspect of data handling. This, however, is not the entire picture, especially for data storage. Without the correct application of authorization and authentication, any encryption measures can be rendered ineffective.

The analysed guidance alternated between explicit acknowledgement that authorization (AuthZ) and authentication (AuthN) were required prerequisites to secure storage and the unstated implicit requirement of AuthN's and AuthZ's existence. Both AuthZ and AuthN must be in place for secure storage to function as expected.

This same oversight of irregular guidance also occurs when discussing potential regulatory requirements. As an example, medical and personal data is subject to multiple different levels of oversight, privacy, and data security requirements, depending on location. The potential points of risk are either only acknowledged briefly or implicitly required.

The overhead of cryptographic operations, and its effect on IoT device operation, is as wide as the possibility that IoT presents. Whilst somewhat banal, this exemplifies both the strength and weakness of IoT in the diversity of potential devices. This diversity means that the impact of cryptographic operations on IoT can range from a mild inconvenience to devastating impact on normal operations.

This overhead has been reduced with newer protocols with increased efficiency, and dedicated hardware, although these newer protocols are not without their issues. Newer editions of protocols like HTTP/2 (Belshe et al., 2015) and HTTP/3 (Bishop, 2022) build on a solid foundation with the aim of efficiency. There are also new protocols, like 6LowPAN (Thubert et al., 2017), that have all the benefits and pitfalls due their relative age.

In larger networks focussed on HTTP/SSL traffic, SSL Offload has long been a known computational expense, and the common approach to reduce load on servers is by moving the cryptographic operations to dedicated hardware. A similar approach can occur in edge computing for IoT, where the edge node may be responsible for heavy-duty encryption, with devices using a lighter level of encryption for first-hop communication. This improvement has also moved to general computing, with CPU's implementing dedicated hardware level instruction specifically for encryption – namely the AES-NI instruction set, present on most modern CPU architectures, and specifically released by Intel in 2010 (Gueron, 2010). This hardware acceleration does not remove the requirements around cryptography – it only makes specific types of cryptographic operations faster and more energy efficient.

When analysing the data storage guidance, the same issue appears – the guidance wavers between explicit and implicit requirements. Generally, when seeking to store IoT data on the device, hardware backed secure storage is the preferred approach described. This presents an immediate issue of sourcing fit for purpose hardware backed secure storage, and the type, form, and functions of the hardware secure storage are not described in detail. That is not to say there is no guidance – the high-level layout and requirements of the secure storage are described in detail; it should be a dedicated, isolated, and physically tamper-proof (or at least tamper resistant) processor and storage that is only accessible via dedicated API's from the main storage and operating system. Given that IoT devices are designed for purpose, this may be sufficient – although a large degree of trust is now transferred to the manufacturer to implement such systems correctly and inform end-users of their usage requirements.

6.1.5 Endpoint Management

Endpoint management is not solely associated with IoT devices; however, it addresses some of the dynamic challenges for IoT that are also present in traditional cybersecurity management. Given that most IoT devices will contain more than one communication endpoint (usually, at a minimum, one data and one management connection), tracking and managing these endpoints at scale would require some level of abstraction. Abstracting the communication security away from individual devices and focussing on a collection of endpoints allows for the capture of the non-traditional communication channels that IoT can take advantage of, and which may not integrate into routine monitoring or security systems. This abstraction away from individual IoT devices also means that each endpoint's usage or role can be managed according to the requirements of the data or access present via the endpoint.

6.1.6 Cybersecurity Policies

Policies are highly interpretative and are tailored to suit the needs of organisations. As each organisation is unique, the associated polices may also be unique, making specific guidance for every situation impractical. As such, guidelines backed by technical referencing can alleviate this issue, by presenting the types of policies and their expected outcomes – with the technical backing to allow for policy writers to make an informed enough decision about the contents and expected outcomes of a given policy.

6.1.7 Device Reset and Refresh

Device reset and refresh form a part of a device's lifecycle, and ties into mobile device management – a well understood hurdle for cybersecurity, with a multitude of tools to manage all types of devices. These tools are generally adapted for traditional computing, centralising the needed functions to ascertain what devices exist, which personnel they are allocated to and where they located both physically and logically, along with any metadata required, like access keys. An accepted facet of this type of centralised management is the ability to reset or refresh devices remotely.

There is an important distinction to be made between *reset* and *refresh*. A *reset* is to reset the device, back to factory defaults, as if the device was just produced. When correctly implemented, this also removes all traces of the device from associated tracking systems and purges all associated data about the user and the device from any backend systems – be they cloud based or otherwise. A *refresh* is not resetting and purging all data but can be construed as a partial reset – targeting on the device configuration and operating system files but leaving any other configurations or files alone.

6.1.8 Strong Defaults

Many cybersecurity incidents occur due to default settings that are never changed or updated when a device is provisioned. Given the nature of IoT devices, the provisioning process may not be interactive or may preclude the ability to update defaults. When defaults must be used, they should be strong defaults. What exactly constitutes a strong default will vary wildly based context of the device – much like cryptography, context will drive the sliding scale of security measures.

6.1.9 Secure Provisioning and Updates

Secure update services are a mainstay of modern operating systems. All the large operating systems such as Windows, MacOS, and Unix/Linux, have some form of update dissemination and verification that is backed by cryptographic signatures. These approaches are not always suitable for IoT devices, and the overall approach of incremental security updates may not always be technically possible for an IoT device, like a NFC tag. For firmware updates, there are three main approaches; one-time programmable, blob update and asset based.

For devices that are never to be updated or are designed as disposable, a one-time programmable approach is taken – the firmware for the device is isolated to a read-only storage medium and cannot be overwritten – if a device ever needed updating it is physically impossible and a new version of the device must be purchased instead. This method relies on the device being secure at all stages of the supply chain.

The blob update model requires an overwritable firmware storage and updates the entire firmware in an all-or-nothing fashion. This approach is common in modern systems, especially those with multiple embedded processors or expansion cards – especially when dealing with proprietary hardware.

The final approach is an asset-based approach, where each area of the device is divided into an asset, with the resultant firmware updating only a single aspect of the device. This is also commonly used in most modern operating systems.

To perform either blob or asset updates remotely and securely, provisioning must incorporate in the fundamentals of CIAAN and cryptographic verification of both source, destination, and payload. As a list of requirements - the update action must be performed by an authenticated and authorised user; the updated files must be delivered in a secure fashion; the files themselves must be verified as complete and unmolested and the device must be able to report and recover from a failed upgrade.

6.1.10 No Usage of Deprecated Protocols

Protocols follow the same cycle of update and improvement as software, albeit generally at a slower pace. This slower pace means that protocol changes usually denote generational leaps, instead of incremental improvements. The requirement for most protocols to be backwards compatible means that even if a device supports the latest protocols, it will also need to support the older generation of protocols. This legacy support is not always possible, as legacy protocols are occasionally removed or deliberately disabled for security (or other) reasons.

6.1.11 Event Logging and Auditing

Event logging and auditing is strongly covered in the analysed documents, with extensive references to the existing body of knowledge, to aid in identification of what events need to be logged, standard formats, and SIEM integration to allow for analytics, alerting and incident recovery.

6.1.12 Hardware Secure Storage

The usage of hardware secure storage has been discussed in earlier sections; however, the usage of hardware secure storage is only one part of secure data storage for IoT. Relying on hardware implementation for cryptographic operations allows for increased efficiency and reliability – at the cost of reliance on specific hardware. As hardware is not guaranteed to be identical, with differing interconnections, functions, and specifications, manufacturers play a delicate and fragile game of integration, where a major error may see end-users confronted with unsolvable hardware issues.

Such ‘low level’ hardware issues are difficult to solve. Indeed, they may not be solvable and where they are, the solutions usually incur a noticeable performance overhead (Carvalho et al., 2014; Lipp et al., 2018). The parasitic computation when mitigating hardware issues makes the software-based encryption for IoT even less feasible due to the increased computation on an already constrained device. These constraints are more common in constrained devices, where efficiency is a key concern – the hardware and firmware APIs are often in ‘lockstep’ with one-another, designed as a single purpose device. This tight integration does not mean that either (hardware or software) is without flaws – both are created by people, and thus, fallible.

Encryption has some applications where the non-technical users understand and desire it. A simple example of this is online banking, where a layperson will understand why they need that application to be secure. This translates to a potential for understanding why something should exists, but not the technical knowledge to differentiate between a poor or strong cryptographic implementation.

This issue of hardware support is not a new issue. Vendor ‘lock-in’ and hardware availability of critical systems is a known problem for most ICT hardware. As an example, common fear is that a mission critical piece of hardware – for example a storage RAID card would malfunction, and the card cannot be sourced anymore, resulting in a complete loss of all data that managed by that hardware. Despite this, the process of ‘vendor lock-in’ still occurs, due to the advantages that it can bring to business operations – reduced complexity, support agreements and business benefits.

The same benefits apply to IoT devices, as they are an extension of the existing ICT operations. There are additional aspects that must be considered for IoT, like the attachment to possible physical interactions. Overall, the existing body of knowledge and toolset deals well with hardware secure storage in IoT, as the issues are no different to other ICT hardware.

6.1.13 Authentication and Authorization

The principles of authentication and authorization do not change between IoT and the existing body of knowledge for traditional computing. The current best-practice implementation of MFA/2FA or AUTHZ and AUTHN mechanisms also generally work well on IoT devices. Following the current best practice for MFA and using the latest protocols (e.g., OAuth2).

6.2 NIST Traditional Cybersecurity Functions

Each function in the NIST industry baseline addresses a key aspect of cybersecurity. Each function is addressed in order they appear in the NIST industry baseline document – Identify, Detect, Respond and Recovery. When addressing each function specific by the NIST industry baseline, a mapping of NIST industry baseline to IoT capabilities is used to highlight the gaps, omissions, and coverage of the NIST industry baseline in comparison to the IoT Capabilities. Where the NIST baseline document adequately covers the application of cybersecurity to IoT, the action will be specifically noted as requiring no additional adaptation for IoT.

Each function is further broken into sub-categories. As an example, the function of 'Protect' contains the categories of Identity Management and Access Control, Awareness Training, Data Security, Information Protection Processes and Procedures, Maintenance and Protective Technology. Finally, each category is broken into specific, actionable sub-categories. Table 130 shows an overview of this breakdown.

Table 130: NIST Framework Function, Category and Code Overview

NIST Function	Sub-Category	Unique ID	Example Code
Identify (ID)	Asset Management	AD	ID.AM-1
	Business Environment	BE	ID.BE-1
	Governance	GV	ID.GV-1
	Risk Assessment	RA	ID.RA-1
	Risk Management Strategy	RM	ID.RM-1
	Supply Chain Risk Management	SC	ID.SC-1
Protect (PR)	Identity Management and Access Control	AC	PR.AC-1
	Awareness and Training	AT	PR.AT-1
	Data Security	DS	PR.DS-1
	Information Protection Processes and Procedure	IP	PR.IP-1
	Maintenance	MA	PR.MA-1
	Protective Technology	PT	PR.PT-1
Detect (DE)	Anomalies and Events	AE	DE.AE-1
	Security Continuous Monitoring	CM	DE.CM-1
	Detection Processes	DP	DE.DP-1
Response (RS)	Response Planning	RP	RS.RP-1
	Communications	CO	RS.CO-1
	Analysis	AN	RS.AN-1
	Mitigation	MI	RS.MI-1
	Improvements	IM	RS.IM-1
Recovery (RC)	Recovery Planning	RP	RC.RP-1
	Improvements	IM	RC.IM-1
	Communications	CO	RC.CO-1

6.2.1 Function: Identify

Identity is a cornerstone of cybersecurity. A large part of interaction with security systems is proving identity through a variety of means. While the Identity category is the NIST Function, it most closely ties to the Confidentiality category in the CIA triangle (Section 2.5.1.1). Without knowing what assets you have (be they physical, digital or data), to whom they belong, who is responsible for them and who is permitted access to them, it becomes problematic to apply meaningful cybersecurity across an organisation. The *Identity* function is impacted by the business units of an organisation and its approach to both risk assessment and management – showcased by the way NIST has defined this function "…Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organisation to focus and prioritise its efforts…" (National Institute of Standards and Technology, 2018, p.7).

Both the NIST IoT Core Capabilities and the 'Trusted Industry Benchmark' agree on the need for strong identification. In traditional networks, identification tooling and management systems have had time to mature and become more integrated into the broader ecosystem of administrative and security processes. The IoT ecosystem has not had the same amount of time and thus suffers from immature tooling. This immaturity compounds the issues, made further still more difficult due to the potential device count and possible lack of direct human interfaces.

This function (Identity, ID) contains the Sub-Categories of Asset Management (AM), Business Environment (BE), Governance (GV), Risk Assessment (RA), Risk Management Strategy (RM) and Supply Chain Risk Management (SC). An example of this coding system is ID.AM-3, which specifies the function 'Identity', Sub-Category 'Asset Management', action number '3'.

6.2.1.1 *NIST Sub-Categories to Findings Mappings*

Table 131 demonstrates the links between the NIST Function of Identity, mapping each of its sub-categories to the IoT Capabilities identified from the analysis of guidance (5.4.7).

Table 131: NIST Identity Function to IoT Capabilities

NIST Function: Identity	NIST IoT Capability
Asset Management	Logical / Physical Identifiers
Business Environment	Not Present
Governance	Not Present

Risk Assessment	Not Present
Risk Management Strategy	Not Present
Supply Chain Risk Management	Not Present

6.2.1.2 *Asset Management (AM)*

Asset Management is a continual and ongoing process to track and catalogue the location and importance of every piece of equipment, data, or other resources within an organisation. Generally, an asset can be described as any data, device or components of the environment that support an information related activity. This covers data, hardware, software, physical objects, specialised facilities, and people.

6.2.1.2.1 System Inventory (NIST ID.AM-1)

System Inventory aims to take note of all physical assets and maintain them in a register. This is complicated by the myriad of different unique identifiers that physical assets will utilise – some complex physical assets will have more than one asset that identifies individual parts within them. A prime example of these multiple identifiers is an automobile – the engine will be tagged with a VIN, and the vehicle will have a licence plate that identifies it for registration, with the potential for more identifiers for other purposes, like serial numbers on individual parts.

6.2.1.2.2 Software Inventory (NIST ID.AM-2)

The software inventory process can be translated (or expanded) directly to include IoT devices. The expansion would be to the data captured during the software inventory process. As IoT devices are not guaranteed to run complex introspections, part of any documentation procedure should also capture the version of embedded services, including firmware. Attempting to individually access and confirm the version of an IoT device would be potentially prohibitive in human resource and time costs. However, a software inventory is especially useful when urgent security patching is required, allowing targeted updates to required devices.

6.2.1.2.3 Communication Dataflow Mapping (NIST ID.AM-3)

ID.AM-3, Communication Dataflow Mapping requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.1.2.4 External System Mappings (NIST ID.AM-4)

ID.AM-4 External System Mapping requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques. Scrutiny should be applied to any cloud integrations focussed on IoT, generally due to their 'newness' in offering, compared to already established cloud offerings.

6.2.1.2.5 Resource Criticality Prioritization (NIST ID.AM-5)

Assessing an IoT device to determine resource criticality prioritisation should include the device itself and the physical actions that can be triggered from the IoT device - if such actions exist. This creates a possible situation where a device in a standalone fashion would is classed as low or negligible risk; however, the physical actions it could take (e.g., opening a floodgate) would be classed as catastrophic. Therefore, the result of any criticality prioritisation assessment must consider both attributes.

6.2.1.2.6 Workforce Cybersecurity (NIST ID.AM-6)

Workforce cybersecurity efforts will need to expand to cover the increase in the numbers of devices that IoT deployments bring. This increase is on top of the established multiplicative effects of BYOD, smartphones, and tablets on device management, tracking, and the associated cybersecurity efforts.

6.2.1.3 *Business Environment (BE)*

Business Environment refers to the 'standard' cybersecurity strategic policies, procedures, and directions that are assumed to exist as part of an organisations robust cybersecurity approach.

6.2.1.3.1 Supply Chain Role Identification (NIST ID.BE-1)

ID.BE-1, Supply Chain Role Identification, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.1.3.2 Service Delivery Dependencies (NIST ID.BE-2)

ID.BE-2, Service Delivery Dependencies, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.1.3.3 Critical Service Dependency Analysis (NIST ID.BE-3)

ID.BE-3, Critical Service Dependency Analysis, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.1.3.4 Critical Infrastructure Resilience (NIST ID.BE-4)

The requirements to recover from an incident or interruption of any type falls under the aegis of Disaster Recovery Planning. Typically, critical infrastructure is a focal point of these plans, and the critical infrastructure is usually a small subset of known assets. Subsequently, these plans account for potential fails states – ensuring that the organisation can still operate in a degraded state during a failure of any type. IoT links a new aspect to networks – the proliferation of physical interactions actions by networked devices.

6.2.1.3.5 Operational Resilience Planning (NIST ID.BE-5)

ID.BE-5, Operational Resilience Planning, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.1.4 *Governance (GV)*

The ability for an organisation to ascertain its overall readiness in governance can be a difficult task, as cybersecurity governance is still relatively new (De Bruin & von Solms, 2016); IoT will only spur additional work to account for the differences between traditional guidance and the unique requirements of IoT. Furthermore, the long-standing outlook of documenting, implementing, and enforcing internal policy and procedures that ensure an organisation adheres to its regulatory, legal, environmental, operational, and risk-based requirements is complicated due to the specialised knowledge requirements across multiple fields of study. Coupling this knowledge requirement with competing goals, requirements, and internal politics creates additional complexities for IoT to establish its own governance within an already complex structure.

6.2.1.4.1 Established Cybersecurity Policies (NIST ID.GV-1)

IoT must have its own governance goals and not be directly subsumed by existing policies. This is important for IoT and Bring-Your-Own-Device (BYOD), as BYOD shares characteristics with IoT and there is an attractiveness to treat them the same and be done with the process. This is erroneous, as while some principles are shared across IoT to BYOD, there are enough differences that this will cause issues in the greater application of cybersecurity.

6.2.1.4.2 Cybersecurity Roles & Responsibilities (NIST ID.GV-2)

ID.GV-2, Cybersecurity Roles & Responsibilities requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.1.4.3 Cybersecurity Regulatory & Legal Responsibilities (NIST ID.GV-3)

ID.GV-3, Cybersecurity Regulatory & Legal Responsibilities requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.1.4.4 Governance & Processes (NIST ID.GV-4)

ID.GV-3, Governance & Processes requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.1.5 *Risk Assessment Strategy (RA)*

Risk assessment is an essential aspect of resource allocation and prioritisation. As such, the core principles of risk assessment can be translated directly from traditional networks and techniques to IoT. However, there are additions needed to cater for IoT and its unique aspects. These unique aspects are across the entire IoT ecosystem – the scale of deployments, domain-specific knowledge requirements, and linking the physical world to digital controls. These alterations may lead to new models or expansion of existing modules to assess risk (Radanliev et al., 2018).

6.2.1.5.1 Asset Vulnerabilities (NIST ID.RA-1)

ID.RA-1, Asset Vulnerabilities, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.1.5.2 Cyber Threat Intelligence (NIST ID.RA-2)

ID.RA-2, Cyber Thread Intelligence, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.1.5.3 Threat Analysis and Documentation (NIST ID.RA-3)

ID.RA-3, Threat Analysis and Documentation, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.1.5.4 Business Impact Analysis (NIST ID.RA-4)

ID.RA-4, Business Impact Analysis, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.1.5.5 Risk Assessment Methodology (NIST ID.RA-5)

ID.RA-5, Risk Assessment Methodology, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.1.5.6 Risk Responses (NIST ID.RA-6)

ID.RA-5, Risk Responses, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.1.6 *Risk Management Strategy (RM)*

A risk of management strategy is a structured, coherent approach to identifying, managing, and assessing risk. It creates a process for the regular review and update of a risk assessment, altering actions and documentation on new developments.

6.2.1.6.1 Risk Management Processes (NIST ID.RM-1)

ID.RM-1, Risk Management Process requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.1.6.2 Risk Tolerance (NIST ID.RM-2)

ID.RM-2, Risk Tolerance requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.1.6.3 Situational Risk Tolerance (NIST ID.RM-3)

ID.RM-3, Situational Risk Tolerance requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.1.7 *Supply Chain Risk Management (SC)*

Supply chain management shares the need for specific additions to cater to IoT with Risk Assessment Strategy. The core principles of supply chain risk management are translatable from traditional cybersecurity to IoT with minimal change. The additions for IoT are focused on the tightly coupled and embedded nature of software for an IoT device. Traditional computing devices generally do not have a difficult upgrade path for embedded firmware or software (outside specialised devices). However, with their low powered nature, IoT devices couple both the software supply chain and hardware supply chain into one. Before IoT, analysis proceeded assuming that they were (generally) isolated chains (Z. Zhu et al., 2021).

6.2.1.7.1 Supply Chain Risk Management Process (NIST ID.SC-1)

ID.SC-1, Supply Chain Risk Management, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.1.7.2 Supplier Assessment (NIST ID.SC-2)

ID.SC-2, Supplier Assessment, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.1.7.3 Routine Assessments (NIST ID.SC-3)

ID.SC-3, Routing Assessments, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.1.7.4 Response and Recovery (NIST ID.SC-4)

ID.SC-4, Supplier Assessment, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.2 Function: Protect

The Protect function aims to reduce and contain effects of a given cybersecurity event. The bulk of these protections are situated outside of an IoT specific network. Given that the bulk of the protections are not specific to IoT, the base principles and approaches from the existing body of knowledge are still applicable and are translatable with minimal adaptation. The specific adaptations for IoT networks will need to adapt for limited and immature toolsets, rapidly evolution ecosystems and lack of standardisation.

This function (Protect, PR) contains the Sub-Categories of Identity Management and Access Control (AC), Awareness and Training (AT), Data Security (DS), Information Protection Processes and Procedures (IP), Maintenance (MA) and Protective Technology (PT). An example of this coding system is PR.AT-3, which specifies the Function 'Protect, Sub-Category 'Awareness and Training', action number '3'.

6.2.2.1 *NIST Sub-Categories to Protect Function Mappings*

Table 132 demonstrates the links between the NIST Function of Identity, mapping each of its sub-categories to the IoT Capabilities identified from the analysis of guidance (5.4.7).

Table 132: NIST Identity Function to IoT Capabilities and Research Findings

NIST Function: Protect	NIST IoT Capability
Identity Management and Access Control	Secure Software Configuration, Secure Interface Management
Awareness and Training	Not Present

Data Security	Secure Data Storage / Transmission, Secure Interface Management
Information Protection Processes and Procedures	Not Present
Maintenance	Secure Update Mechanism
Protective Technology	Not Present

6.2.2.2 *Identity Management, Authentication and Access Control*

IoT changes some of the identity requirements in cybersecurity, which is the domain of 'proving you are whom you say you are' to encompass devices and machine-to-machine and API-to-API communications at scale. Access controls encompass and rely on authentication and identity management. There are also implicit requirements to apply access controls, like authorisation. This decoupling of identity to encompass devices does not create new techniques, but it requires that management tools and procedures now account for a device and its associated attributes, lifecycles, and metadata.

6.2.2.2.1 Identity & Credential management (NIST PR.AC-1)

IoT devices will generally follow one of two approaches to access controls. Centralisation, via a management layer; or standalone, with each device responsible for its access. Each has its own unique issues – centralised systems are generally RBAC and have an issue at scale from the overhead, especially in highly dynamic environments; whereas standalone devices are generally isolated from any management tooling, requiring shared credentials or other potentially insecure access schemes for shared access.

6.2.2.2.2 Physical Access Restrictions (NIST PR.AC-2)

Physical protection of IoT devices requires minimal expansion of traditional techniques. Generally, IoT devices should be considered as always accessible, as they are usually small and isolated devices. Conceivably, these can be physically touched at any point by a malicious actor. They are also difficult to track – wireless tracking is not perfect and has an area of effectiveness.

6.2.2.2.3 Remote Access Restrictions (NIST PR.AC-3)

PR.AC-3, Remote Access Restriction, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.2.2.4 Resource Access and Authorisation (PR.AC-4)

PR.AC-4, Resource Access and Authorisation, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.2.2.5 Network Integrity (NIST PR.AC-5)

PR.AC-5, Network Integrity, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.2.2.6 Identity Binding (NIST PR.AC-6)

Identity binding in IoT will be significantly affected by the technology and approach used to secure the devices. As an example, utilising blockchain as the underlying authentication mechanism will change how identity is managed and pinned to a specific device or user. The mechanisms will be varied, however, the core principles of identity binding can be translated across from traditional cybersecurity with minimal adaptation; assuming knowledge of the potential affects that an IoT specific approach or technology will have on the greater ecosystem.

6.2.2.2.7 Scaled Authentication Measures (NIST PR.AC-7)

PR.AC-7, Scaled Authentication Measures, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.2.3 *Awareness and Training (AT)*

The existence of awareness and training programs and their associated policies and procedures should have specific content for IoT in addition to the already existing content that is presumed to exist.

6.2.2.3.1 General User Training (NIST PR.AT-1)

Precisely what constitutes general user training changes from organisation to organisation, dependant largely on the resources allocated to ongoing cybersecurity measures and training. The principle of having ongoing user training of the business processes, policies and procedures remains unchanged for IoT.

6.2.2.3.2 Privileged Users Roles and Responsibilities (NIST PR.AT-2)

PR.AT-2, Privileged Users Roles and Responsibilities, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.2.3.3 Third-Party User Roles and Responsibilities (NIST PR.AT-3)

PR.AT-3, Third-Party User Roles and Responsibilities, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.2.3.4 Executive Roles and Responsibilities (NIST PR.AT-4)

PR.AT-4, Executive Roles & Responsibilities, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.2.3.5 Physical and Cyber Security Roles (NIST PR.AT-5)

PR.AT-5, Physical and Cyber Security Roles, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.2.4 *Data Security (DS)*

Data security measures, like access controls, encrypted data and auditing systems are presumed to exist as part of a robust cybersecurity approach.

6.2.2.4.1 Data At Rest (NIST PR.DS-1)

PR.DS-1, Data At Rest, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.2.4.2 Data In Transit (NIST PR.DS-2)

PR.DS-2, Data In Transit, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques – barring the awareness of IoT specific protocol limitations.

6.2.2.4.3 Asset Management Process (NIST PR.DS-3)

PR.DS-3, Asset Management, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.2.4.4 Sustained Availability (NIST PR.DS-4)

PR.DS-4, Sustained Availability, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.2.4.5 Data Leak Protection (NIST PR.DS-5)

PR.DS-5, Data Leak Protection, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.2.4.6 Software Integrity Checks (NIST PR.DS-6)

PR.DS-6, Software Integrity Checks depends heavily on the hardware capabilities of a given IoT device. Most guidance requires the usage of a dedicated security processer, analogous to a desktop TPM, to take the place of software-level encryption. Some guidance explicitly forbids the usage of software-based cryptography for secure storage applications. Other well-known and established techniques from the existing body of knowledge can be translated directly for IoT.

6.2.2.4.7 Development Environment Isolation (NIST PR.DS-7)

PR.DS-7, Development Environment Isolation, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.2.4.8 Hardware Integrity Checks (NIST PR.DS-8)

PR.DS-8, Hardware Integrity Checks, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.2.5 *Information Protection Processes and Procedures (IP)*

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organisational entities), processes, and procedures are maintained and used to manage the protection of information systems and assets.

6.2.2.5.1 Baseline Configuration (NIST PR.IP-1)

PR.IP-1, Baseline Configuration, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.2.5.2 System Development Life Cycle (NIST PR.IP-2)

PR.IP-2, System Development Life Cycle, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.2.5.3 Configuration Change Control (NIST PR.IP-3)

PR.IP-3, Configuration Change Control, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.2.5.4 Backups (NIST PR.IP-4)

PR.IP-4, Backups, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.2.5.5 Physical Operational Environment Requirements (NIST PR.IP-5)

PR.IP-5, Physical Operational Environment Requirements, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.2.5.6 Data Destruction (NIST PR.IP-6)

PR.IP-6, Data Destruction, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.2.5.7 Process Improvement (NIST PR.IP-7)

PR.IP-7, Process Improvements, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.2.5.8 Shared Effectiveness (NIST PR.IP-8)

PR.IP-8, Shared Effectiveness, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.2.5.9 Response Plans (NIST PR.IP-9)

PR.IP-9, Response Planning, requires no additional adaptation for IoT and can be translated directly from traditional networks and techniques.

6.2.2.5.10 Active and Simulation Testing (NIST PR.IP-10)

PR.IP-10, Active and Simulation Testing, requires particular attention to attached devices and their potentially obscure knock-on effects. The existing body of knowledge can be translated directly with this caveat.

6.2.2.5.11 Human Resources Cybersecurity Integration (NIST PR.IP-11)

PR.IP-11, Human Resources (HR) Cybersecurity Integration, requires minimal changes for IoT. HR staff should be exempt from overall training as prescribed in 6.2.2.3.1 General User Training (NIST PR.AT-1). HR specific training to target organisational goals and approaches to IoT should expand on the generalised training.

6.2.2.5.12 Vulnerability Management Plan (NIST PR.IP-12)

PR.IP-12, Vulnerability Management Plan, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.2.6 *Maintenance (MA)*

Maintenance of IoT in literature focuses on utilising IoT to monitor and maintain other devices.

6.2.2.6.1 Maintenance and Repair (NIST PR.MA-1)

PR.MA-1, Maintenance and Repair, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.2.6.2 Remote Maintenance Auditing (NIST PR.MA-2)

PR.MA-2, Remote Maintenance Auditing, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.2.7 *Protective Technology (PT)*

Protective technology is the overall incorporation of technologies to aid cybersecurity and the resilience of systems. This integration requires adherence to the related policies, procedures and agreements that coincide with the technological protections.

6.2.2.7.1 Auditing Process (NIST PR.PT-1)

PR.PT-1, Auditing Process, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.2.7.2 Removable Media Restrictions (NIST PR.PT-2)

PR.PT-2, Removable Media Restrictions, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.2.7.3 Principle of Least Functionality (NIST PR.PT-3)

PR.PT-3, Principle of Least Functionality, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.2.7.4 Communication and Control Network Restrictions (NIST PR.PT-4)

PR-PT-4, Communication and Control Network Restrictions, requires minimal adaptation for IoT and can be translated directly, considering that IoT specific protocols may require significant additional work.

6.2.2.7.5 Implementation of Resilience Technologies (NIST PR.PT-5)

Considering the above stated caveats, the existing body of knowledge can be translated across.

6.2.3 Function: Detect

The detection of security-related events is expected to exist as part of existing robust cybersecurity measures. This function (Detect) contains the Sub-Categories of Asset Management (AM), Business Environment (BE), Governance (GV), Risk Assessment (RA), Risk Management Strategy (RM) and Supply Chain Risk Management (SC). An example of this coding system is ID.AM-3, which specifies the Function ‘Identity’, Sub-Category ‘Asset Management’, action number ‘3’.

6.2.3.1 *NIST Sub-Categories to Detect Function Mapping*

Table 133 demonstrates the links between the NIST Function of Identity, mapping each of its sub-categories to the IoT Capabilities identified from the analysis of guidance (5.4.7).

Table 133: NIST Detect Function to IoT Capabilities and Research Findings

NIST Function: Detect	NIST IoT Capability
Anomalies and Events	State Awareness
Security Continuous Monitoring	State Awareness
Detection Processes	State Awareness

6.2.3.2 *Anomalies and Events*

The detection of anomalies and events is common practice for cybersecurity. IoT is an opportunity to expand this capability, with detailed reporting of physical devices at scale made possible with the use of IoT devices. There is a dearth of information covering detecting anomalies within IoT devices. Instead, the focus is on the application of IoT to monitoring other objects or devices. This lack of information opens a large area of future work to detect and monitor events within IoT networks and devices.

6.2.3.2.1 Baseline Expected Network Operation (NIST DE.AE-1)

DE.AE-1, Baseline Expected Network Operation, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.3.2.2 Analysis of Detected Events (NIST DE.AE-2)

DE.AE-2, Analysis of Detected Events, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.3.2.3 Event Correlation (NIST DE.AE-3)

DE.AE-3, Event Correlation, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.3.2.4 Event Impact (NIST DE.AE-4)

DE.AE-4, Event Impact, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.3.2.5 Alert Thresholds (NIST DE.AE-5)

The threshold for what constitutes a missing device will need to be tailored per IoT device, accounting for deployment characteristics, criticality, and associated business processes – and exactly when a device is 'missing' instead of 'not communicating'. Some IoT devices are not designed to have a permanent network presence – as such, an active polling system for presence will potentially cause false positives by marking a sleeping IoT device inactive. Ideally, IoT monitoring systems can utilise a check-in delta, where the metric is 'time device last seen'. All other principles from the established body of knowledge can be translated without additional adaptation for IoT.

6.2.3.3 *Security Continuous Monitoring*

The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. This includes monitoring both the physical and digital presence of all devices, staff, users, and programs – this includes ongoing identification of new vulnerabilities found in software.

6.2.3.3.1 Network Monitoring (NIST DE.CM-1)

The principles of networking monitoring are not changed by the introduction of IoT – instead, there are unique challenges presented by IoT devices that must be addressed. The diversity of IoT protocols, device types, and communication mediums complicate the aggregation of monitoring to a single point. This aggregation is further complicated by the usage of publish-subscribe modules, instead of traditional TCP/IP bi-directional connections, and the introduction of 'edge' and 'fog' computing, creating additional aggregation points.

6.2.3.3.2 Physical Monitoring (NIST DE.CM-2)

DE.CM-2, Physical Monitoring, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.3.3.3 Personnel Monitoring (NIST DE.CM-3)

The inadvertent inclusion of IoT devices by a staff member due to unawareness of IoT can create a potential omission in device monitoring. Barring this awareness, DE.CM-3, Physical Monitoring, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.3.3.4 Malware Detection (NIST DE.CM-4)

Traditional antiviral and active scanning techniques are not directly compatible with IoT. The overhead involved with active scanning and live code analysis is not congruent with low powered longevity. The current guidance combines the existing technologies that protect networks before requiring protections on the devices – intrusion detection/prevention systems, monitoring and anomaly detection are the primary measures.

6.2.3.3.5 Unauthorised Mobile Code (NIST DE.CM-5)

Mobile code has been broadly scoped as any code that can be transmitted and subsequently executed on an IoT device. This broad scope requires that all decisions for the restriction of any mobile code are based on an organisation's specific systems and the analysis of potential harm. As IoT allows a multitude of new and complex situations, there is significant difficulty in adequately capturing what protections are required.

There is also an advantage, in that the limitations imposed due to the characteristics of IoT also limit the pool of potential protection mechanisms. As such, IoT will tend to rely on code signatures and chains of trust, as these types of checks can be performed at runtime and are scalable in strictness. The detection of code that does not adhere to such protection types will rely on monitoring and alerting systems that are assumed to exist as part of a robust cybersecurity approach.

6.2.3.3.6 External Service Monitoring (NIST DE.CM-6)

DE.CM-6, External Service Monitoring, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.3.3.7 Unauthorised Entity Monitoring (NIST DE.CM-7)

Unauthorised entity monitoring mixes multiple, distinct, and complex items under the umbrella of an 'entity'. Software, devices, people, and device actions all require vastly different monitoring solutions when isolated; it is highly unlikely that a single solution would cover each categories' requirements. This concealment of complexity is detrimental to isolating the interrelations that can occur between the areas. The existing body of knowledge caters to these areas and can be translated with minimal adaptation for IoT.

6.2.3.3.8 Vulnerability Scanning (NIST DE.CM-8)

DE.CM-8, Vulnerability Scanning, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.3.4 *Detection Processes*

Detection processes and procedures are maintained and tested to ensure awareness of anomalous events. This section will cover the roles, responsibilities, requirements, testing, communications, and refinement expectations of detection processes.

6.2.3.4.1 Roles & Responsibilities (NIST DE.DP-1)

DE.DP-1, Roles and Responsibilities, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.3.4.2 Detection Requirements (NIST DE.DP-2)

DE.DP-2, Detection Requirements, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.3.4.3 Detection Testing (NIST DE.DP-3)

DE.DP-4, Detection Testing, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.3.4.4 Detection Event Communication (NIST DE.DP-4)

DE.DP-5, Detection Event Communication, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.3.4.5 Continual Refinement (NIST DE.DP-5)

DE.DP-5, Continual Refinement, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.4 Function: Respond

A robust set of response plans should already exist as part of standard business practices. These plans aim to reduce the impact of any cybersecurity related event. This function (Respond) contains the sub-categories of Response Planning (RP), Communications (CO), Analysis (AN), Mitigation and Improvements. An example of this coding system is RS.CO-4 which specifies the Function 'Respond', Sub-Category 'Communications', actions number '4'.

6.2.4.1 *NIST Sub-Categories to Respond Function Mappings*

Table 134 presents the links identified between the NIST Function of Detect, and the applicable IoT capabilities identified in the research.

Table 134: Detect Respond to IoT Capabilities and Research Findings

NIST Function: Respond	NIST IoT Capability
Response Planning	Not Present
Communications	Not Present
Analysis	Not Present
Mitigation	Not Present

Improvements	Not Present

6.2.4.2 *Response Planning*

Response planning involves disseminating and utilising processes and procedures associated with detection and response to cybersecurity events. A dedicated response plan aids in expedient recovery to normal operations after an adverse event has occurred.

6.2.4.2.1 Response Plan Utilisation (NIST RS.RP-1)

NIST RS.RP-1, Response Plan Utilisation, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.4.3 *Communications*

Internal and external communication needs differ in scope and requirements, leading to differing priorities and required information. External agencies engaged during incidents (such as CERT teams or law enforcement) will also have specialised communication requirements and prerequisites. These internal and external lines of communications and their associated requirements are to ensure that collaboration and effective responses are coordinated across all parts of the organisation and across organisational lines when required.

6.2.4.3.1 Personnel Roles and Order of Operations (NIST RS.CO-1)

NIST RS.CO-1, Personnel Roles and Order of Operations requires minimal adaptation from that traditional body of knowledge. IoT subject matter experts must be an integral part of constructing and maintaining these communication lines.

6.2.4.3.2 Incident Reporting (NIST RS.CO-2)

NIST RS.CO-2, Incident Reporting, requires no additional adaptation for IoT and can be translated from traditional networks and techniques. Additionally, the IoT environment is under rapid evolution and change, and as such regulatory and reporting mandates are equally likely to shift to in answer to ecosystem changes.

6.2.4.3.3 Information Consistency (NIST RS.CO-3)

NIST RS.CO-3, Information Consistency, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.4.3.4 Stakeholder Coordination (NIST RS.CO-4)

NIST RS.CO-4, Stakeholder Coordination, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.4.3.5 Voluntary Communication with Stakeholders (NIST RS.CO-5)

NIST RS.CO-5, Voluntary Stakeholder Communication, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.4.4 *Analysis*

A post-incident analysis process is expected to exist and conform to an organisation's legal and internal requirements. These processes should support quick and effective responses and underpin recovery efforts. Analysis depends heavily on monitoring and the existence of an auditable trail of events.

6.2.4.4.1 Notification Investigation (NIST RS.AN-1)

NIST RS.AN-1, Notification Investigation, requires no additional adaptation for IoT and can be translated from traditional networks and techniques. The existing onus to investigate and action warnings from monitoring system remains unchanged from traditional networking and techniques.

6.2.4.4.2 Incident Impact (NIST RS.AN-2)

NIST RS.AN-2, Incident Impact, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.4.4.3 Forensic Analysis (NIST RS.AN-3)

NIST RS.AN-3, Forensic Analysis, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.4.4.4 Incident Categorisation (NIST RS.AN-4)

NIST RS.AN-4, Incident Categorisation, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.4.4.5 Vulnerability Disclosure Process (NIST RS.AN-5)

NIST RS.AN-5, Vulnerability Disclosure Process, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.4.5 *Mitigation*

The activities surrounding active mitigation of cybersecurity events – including mitigation of its potentially damaging effects and resolution are expected to exist as part of a robust cybersecurity program.

6.2.4.5.1 Incident Containment (RS.MI-1)

RS.MI-1, Incident Containment, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.4.5.2 Incident Mitigation (RS.MI-2)

RS.MI-2, Incident Mitigation, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.4.5.3 Continual Evaluation (RS.MI-3)

RS.MI-3, Continual Evaluation, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.4.6 *Improvements*

Organisations should undertake detailed retrospectives to ensure that lessons learnt during and after cybersecurity events are incorporated into all relevant policies, procedures, approaches, and disaster plans. This retrospective and continual improvement to internal documents and procedures are expected to exist as part of an existing robust cybersecurity approach.

6.2.4.6.1 Lessons Learned (RS.IM-1)

RS.IM-1, Lessons Learned, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.4.6.2 Update Strategies (RS.IM-2)

RS.IM-2, Update Strategies, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.5 Function: Recovery

This function encompasses the return to normal functionality after a cybersecurity incident. This function (Recovery) contains the sub-categories of Recovery Planning (RC), Improvements (IM), and Communications (CO). An example of this coding system is RC.IM-2, which specifies the Function ‘Recovery’, sub-category ‘Improvements’, action number ‘2’.

6.2.5.1 *NIST Sub-Categories to Recovery Function Mappings*

Table 135 presents the links identified between the NIST Function of Detect, the applicable IoT Capabilities and the associated research findings.

Table 135: Recovery to IoT Capabilities and Research Findings

NIST Function: Respond	NIST IoT Capability
Recovery Planning	Not Present
Improvements	Not Present
Communications	Not Present

6.2.5.2 *Recovery Planning*

Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.

6.2.5.2.1 Recovery Plan Execution (RC.RP-1)

RC.RP-1, Recovery Plan Execution, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.5.3 *Recovery Plan Improvements*

The continual improvement of recovery planning processes is expected to exist as part of a robust cybersecurity approach.

6.2.5.3.1 Lessons Learned (NIST RC.IM-1)

RC.IM-1, Lessons Learned, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.5.3.2 Updating Strategies (NIST RC.IM-2)

RC.IM-2, Updating Strategies, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.5.4 *Communications*

Relations and communication with both internal and external entities is expected to exist as part of a robust cybersecurity approach.

6.2.5.4.1 Public Relation Management (NIST RC.CO-1)

RC.CO-1, Public Relation management, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.5.4.2 Reputation Management (NIST RC.CO-2)

RC.CO-2, Reputation Management, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.2.5.4.3 Recovery Activities (NIST RC.CO-3)

RC.CO-3, Recovery Activities, requires no additional adaptation for IoT and can be translated from traditional networks and techniques.

6.3 SUMMARY

This analysis has identified the significant gaps in current cybersecurity guidance in comparison to the existing body of knowledge for non IoT applications. It has also identified where this existing body of knowledge can be translated to IoT directly, and where modifications or additions of varying degrees are required. The issues identified are both specific to devices and their capabilities, and wider issues that affect the entire IoT ecosystem.

Using the results from this chapter, additional work can be undertaken to target the deficiencies identified in IoT cybersecurity guidance. This work, as with the approach taken with the analysis, would depending on the existing knowledge to minimise the requirement for new guidance, and instead rely on what is already existing – where the existing guidance is acceptable.

7 DISCUSSION

The research has revealed the technical limitations of the current IoT cybersecurity guidance and developed a framework to address these limitations. Given the complicated interrelations between the components of the research, this discussion takes the following form. Firstly, clarification of where the newly developed framework is placed within existing cybersecurity guidance and an overview of its components. Then, a more detailed discussion of the identified issues that are addressed in the newly created framework and a demonstration of how the research framework works to fill the gaps that it identified. Finally, a worked example will demonstrate the practical application of the research framework.

By using the existing body of knowledge as a basis, the 'Trusted Industry Baseline' or 'TIB', which is the Framework for Improving Critical Infrastructure Cybersecurity (National Institute of Standards and Technology, 2018), the security of IoT can be enhanced by building on existing experience and lessons learnt within the field of cybersecurity, instead of attempting to approach IoT cybersecurity as a blank slate.

To take advantage of existing knowledge, the framework acts as an overlay, expanding, modifying, or adding to the existing knowledge to address the issues identified. Whilst the newly created framework can 'stand-alone', it is most effective when paired with the extensive existing body of knowledge. Further, the framework addresses two distinct aspects of IoT – the ecosystem, where the actions are independent of a given device; and technical specifications, where the actions taken will depend on an IoT devices' characteristics and functionality. Figure 31 illustrates the overlay approach, where each layer builds on and expands the Trusted Industry Baseline (TIB). For ease of reference, the technical component is called the IoT Security Overlay Framework (IoTSOF), and the ecosystem component is called the IoTSOF-Ecosystem (IoTSOF-E).

When layering the selected frameworks beneath IoTSOF and IoTSOF-E the inclusion of TIB is not mandatory. The IoTSOF and IoTSOF-E are framework agnostic and will still function without using the TIB as a base, although with potentially diminished effectiveness, as the IoTSoF/E frameworks are designed to work with the Trusted Industry Baseline.

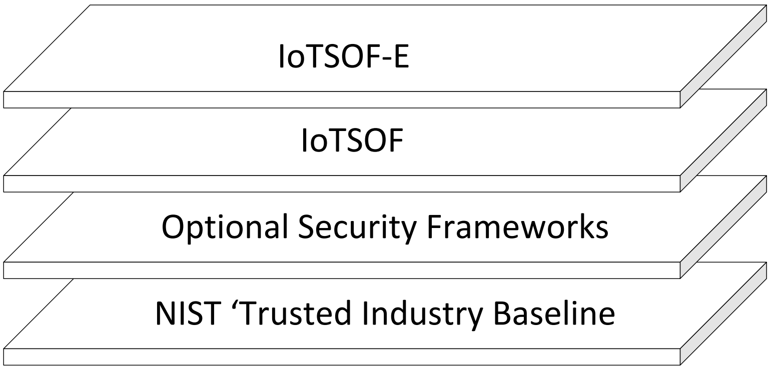


Figure 31: IoT Overlay Framework Construction

The IoTSOF and IoTSOF-E are deliberately constructed to take advantage of the existing body of knowledge and allows for dynamic targeting of actions at both the ecosystem level and the device level. This allows for the framework to extend, modify, or expand on the specific points that need alteration for IoT, without performing unnecessary work where modification or expansion is not necessary. Due to the nature of IoT devices and IoT networks, there are common issues that must be addressed across the ecosystem, no matter the type of IoT device.

The IoTSOF-E is concerned with these broad IoT interactions at a principal level, instead of specific technical controls. However, the IoT ecosystem is intrinsically linked to the details at the ‘lower’ technical level. Just as an aspect of the IoT ecosystem can shape a technical specification, a technical specification can shape an action in the IoT ecosystem. The flow of information is not strictly just from Ecosystem to Device, it can also go from Device to Ecosystem. Without this bidirectional interaction, the IoTSOF/E would fail to account for the dynamic, fractured, and disparate IoT ecosystem. Notably, this framework is *not* an implementation guide; instead, it lays the foundation for implementation guides to address the detailed security requirements for any given IoT deployment.

To use the IoTSOF/E framework(s) in an effective manner, the starting point is the lowest level of the framework – the technical limitations. As the IoTSOF/E frameworks are comprised of technical limitations, and these limitations shape the feasibility of cybersecurity protections. As such, the first step is to identify the technical limitations of a given IoT device. Then, the ecosystem levels aspects of the given deployment can be identified. This is separate to the organisation’s identification of their requirements for implementing the framework.

This back and forth between technical limitations, ecosystem aspects and requirements of the deployment may result in several iterations to identify an approach that meets requirements while addressing technical limitations – this looping decision process is demonstrated in Figure 32. This process of identification of the lowest possible level of technical limitation is required, lest a technical limitation be unaccounted for when determining a larger-scoped approach, causing difficulties when attempting to apply cybersecurity protections to arrive at an acceptable level of residual risk.

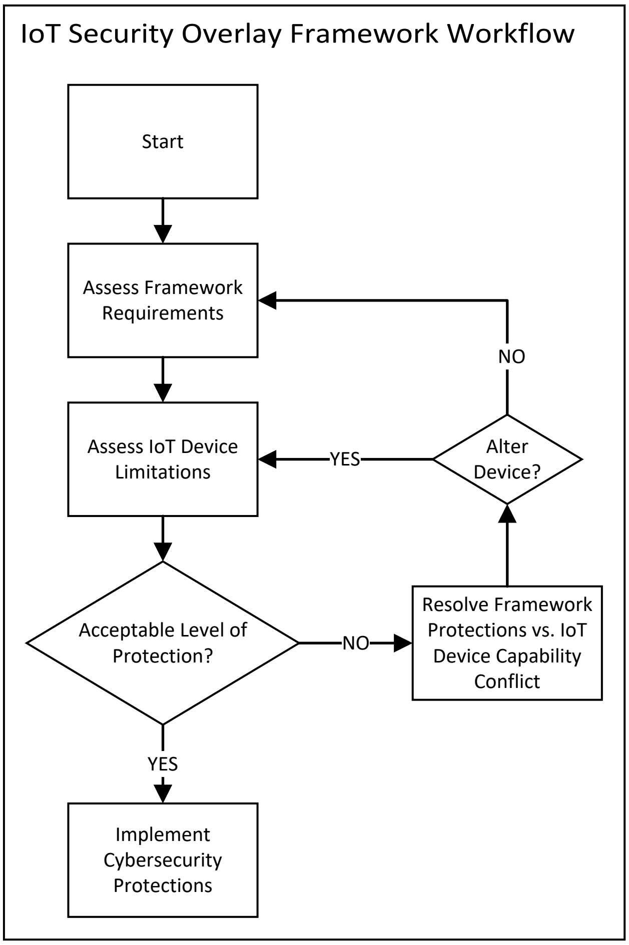

IoT Security Overlay Framework Workflow
Start
Assess Framework Requirements
NO
Assess IoT Device Limitations
YES
Alter Device?
Acceptable Level of Protection?
NO
Resolve Framework Protections vs. IoT Device Capability Conflict
YES
Implement Cybersecurity Protections

Figure 32: IoT Security Overlay Framework Example Workflow

The limitations of the IoT ecosystem are based on the generalised limitations of IoT devices. In line with the IoTSOF's focus of expansion and modification, not all identified ecosystem level issues require discussion, as these points fall within existing, fundamental, cybersecurity practice. An example of such a fundamental point; in Cyber-Physical Systems all assessment of potential device actions should be extended to include the physical interactions the IoT devices can trigger. There is no change to any processes.

7.1 UNIQUE IOT CONSIDERATIONS

There are additional unique security considerations that must be kept 'in mind' when creating, implementing, or analysing IoT cybersecurity. These considerations are loosely coupled to the IoTSOF-E and IoTSOF, in that they are addressed in the framework actions. The points are discussed in the same order as they appear in section 6.1. Additionally, each discussion point is split between 'Ecosystem' (IoTSOF-E) and 'Technical' (IoTSOF) where applicable – not all points of discussion have difference between the technical and ecosystem levels. Specifically, 7.1.1 and 7.1.2 have ecosystem level discussion points, whereas all others are technical only.

7.1.1 Modern Cryptography

Cryptography is a foundational aspect of cybersecurity. As such a pervasive aspect, the issues identified span both the ecosystem and technical level. The need for secrecy is especially important for digital communications, where dedicated protocols and algorithms vetted by mathematicians and dedicated testing have taken the forefront. The modern application for cryptography now relies on the input of thousands of people, with public, open protocols, and ciphers – of which conceivably the most ubiquitous is the OpenSSL Project, the cornerstone of most HTTPS traffic on the internet.

Were there a cybersecurity 'wish list' of 'the best possible cryptography', then, if no constraints otherwise exist, the very best approach would be akin to the following. To use the newest version of a secure protocol, a key with the greatest amount of entropy, from a verified and secure implementation of all cryptographic functions. In practicality, security is a sliding scale and must be applied to the needs of what is to be protected; it is a matter of *when* the cryptographic keys will be broken, not *if*.

To continue along the same vein as the given example – HTTPS traffic is secured by cryptography, but this does not mean that nothing can ever go wrong. Even giants, such as the OpenSSL Project, are not immune to vulnerabilities and issues – the Heartbleed (Carvalho et al., 2014) vulnerability presented a massive issue – it could potentially break all secure traffic and allow decryption of data streams. Potentially, bank transactions were not secret, passwords were decryptable and secure access tokens no longer secure as the cryptography securing these essentially secret bits of information from prying eyes was (potentially) stripped away.

This illustrates the need to create and operate cryptographic measures in a well-guided manner – 'hand-rolling' cryptography, incorrect or insecure implementations and using deprecated algorithms drastically reduce the strength of protection provided. Instead of utilising the tested and secure versions of these algorithms, which have been vetted for both form and function.

7.1.1.1 *Ecosystem*

Modern cryptography is a potentially contentious discussion point for IoT cybersecurity. The nature of IoT devices create unique restrictions and challenges that must be accounted for. The IoTSOF accounts for the restrictions present in IoT devices – however, not everything required alteration. The base principles that drive the need for cryptography are unchanged – ensuring that secret information stays secret and is only visible to the intended recipients. The computation and networking limitations of IoT near universally negate the ability to apply 'heavy' cryptography to all communications, forcing IoT devices and their communication streams to be more circumspect in the application of cryptography. The requirement to limit the computational overheads on IoT devices, however, does not reduce the required rigour for the implementation of cryptographic protections – a flaw in cryptography impacts nearly every aspect of cybersecurity.

7.1.1.2 *Technical*

The IoT ecosystem challenges are made more difficult due to the characteristics of IoT devices, with significant issues potentially arising due to specialised hardware. As IoT devices are specialised hardware, hardware level support for features, especially hardware-backed secure storage, or cryptographic focused application-specific integration circuits (ASIC) is not guaranteed. This makes a device's technical specifications a critical factor when determining the limitations of any specific deployment. This potential for hardware limitation is not restricted to the devices, with IoT specific network architectures also playing a factor – the logical and physical network layout and the protocols used will also affect the potential cybersecurity protections that can be applied.

7.1.2 Secure Data Storage and Transmission

Secure data storage and transmission are intrinsically tied to modern cryptography, as without a sound implementation of cryptography, there is minimal basis for the aspect of secure data storage or transmission – these are linked, as you cannot store everything on the device, nor will it always be feasible to encrypt all communications with an IoT device. This is different to the traditional approach to cybersecurity, where data storage and data transmission are related, but separate.

7.1.2.1 *Ecosystem*

This joint approach to secure data storage and transmission is mainly due to new, specialised IoT protocols and the new approaches to IoT networking enabled by these protocols – namely, 'edge' and 'fog' computing, where targeted offload of tasks adds additional complexity to network design and helps to alleviate the issue of IoT devices' limited compute ability. This complexity in comparison to traditional computing also occurs in secure data storage, where specialised hardware is the primary method to secure data storage, which comes with manufacturer-decided limitations, if it is present at all. An added factor is the dispersion of devices, making the possibility of physical theft somewhat higher than with other types of devices, necessitating additional data protection should the device be physically compromised.

7.1.2.2 *Technical*

The usage of newer protocols for IoT will create a point of contention. IoT protocols are designed to promote the needs of the ecosystem – self-healing, resilient and efficient. Heavy security measures do not always align with these measures, and like all cybersecurity, some form of compromise is required. This is further exacerbated by the breadth of different protocols that cross differing transmission media that live within IoT; ZigBee, Z-Wave, Bluetooth, 6LoWAN, LPWAN – some are wireless mesh protocols, some are wireless pairing protocols, and others are transmission medium agnostic.

This conglomeration of multiple protocols and behaviours is unlikely to integrate cleanly into existing tooling used to monitor traditional networking traffic. To alleviate this, a systematic approach that vets both protocols supported by IoT devices, their aggregation points, the communication medium, and expected behaviour against a desired set of features would be ideal.

7.1.3 Strong Defaults

Weak defaults are a significant factor in security breaches (Coffey, 2017; Fernández-Caramés & Fraga-Lamas, 2020; B. Zhu et al., 2011). Despite this known issue, they are still exploited with regularity. The physical scope of IoT devices makes embedded defaults a much larger attack surface than in traditional computing, due to a combination of scope and potential difficulty in remediation. The IoT device may have an identifier injected by the manufacturer that cannot be changed, or the possible thousands of devices needing manual alteration has the potential to create an immense workload. Some headway has been made by manufacturer embedded secure defaults, like UUID's and random passphrases per device.

7.1.4 Secure Provisioning

Secure provisioning relies heavily on Secure Data Storage and Transmission, as well as Modern Cryptography to function in the expected, secure manner. Oblique attacks against devices, like update poisoning (Levi et al., 2018) are more common, as this type of attack allows a single compromise to be magnified exponentially. IoT devices face additional challenges, as the nature of IoT devices restrict the tooling available for remote provisioning and update management.

In particular, fit for purpose or industry specific Mobile Device Management tooling (*IoT Security Guidelines for IoT Service Ecosystem V2.0*, 2017) is an area where the maturity of process and tooling for IoT provisioning and update management is not yet at parity with traditional computing. This inequality of process and tooling prevents the creation of a generic, single-pane approaches that can incorporate the distinct challenges of IoT. The challenges facing IoT update management tooling are multifaceted, and include direct technical challenges, like network protocol incompatibly, to the more indirect, like the manpower needed to recover potential thousands of scattered IoT devices from a failed update or compromise.

7.1.5 Hardware Secure Storage

Hardware secure storage is a recommended feature in IoT security frameworks, but not all IoT devices are guaranteed to support such advanced functionality. As IoT hardware is specific to each manufacturer, there is potential for software to become locked to a specific piece of hardware, with differences in API or access requirements. It also means that any hardware flaw would difficult to fix, just as CPU's have suffered with Spectre (Chowdhuryy & Yao, 2021) and Meltdown (Lipp et al., 2018), so too could hardware based secure storage suffer from hardware-level vulnerabilities. Despite these limitations, software based secure storage is not always a viable option, and the greater efficiency of using dedicated hardware to offload computationally intensive tasks is of particular interest to computationally constrained IoT devices.

7.1.6 Authentication and Authorization

Authentication (AuthN) and Authorization (AuthZ) are, in principle, still the same as traditional computing. The newer approaches to AuthN and AuthZ that are specifically designed take advantage of the unique aspects of IoT do not invalidate or remove the need for both AuthN and AuthZ within the IoT ecosystem to be secure. The newer approaches, like web-of-trust (Durand et al., 2017), mesh-protocol embedded authentication mechanisms, or offloading of these functions to an aggregation point outside of IoT are being adapted for the challenges in IoT – specifically, the limitations on computation power and networking.

New protocols and adaptations of existing secure protocols create an area where new technology is rapidly developed and deployed. These newly adapted and deployed solutions are still imperfect and have known weaknesses (Nguyen et al., 2015). Notably, this weakens the underpinnings of access control which suffers from its own well understood problems. Role-Based Access Control (RBAC), a mainstay of cybersecurity and organisational user management, has scaling issues, and is not always suitable for application to IoT (Kemmerer, 2003; E.-K. Lee et al., 2017; Thakare et al., 2020). Discretionary Access Control is not used often in large scale networks and Managed Security is firmly established in high confidentiality requirement areas. These established approaches will need adaptation to their application for IoT, as IoT expands the attack surface of an organisation and creates a new physical layer of networking that mandates a new logical approach.

The limitations of modern cryptography, secure data transmission, and secure data storage must be addressed to effectively implement both AuthN and AuthZ. As AuthN requires a secure communication channel to be effective, and without a secure and valid AuthN, AuthZ is compromised, the approach to both AuthN and AuthZ must identify and mitigate the identified issues with cryptography and networking for application for IoT. If these limitations are not identified and addressed, any implementation of AuthN or AuthZ could potentially suffer from vulnerabilities.

IoT aims to solve these issues by stepping away from more traditional access control mechanisms and focusing on utilising the characteristics of IoT as a strength instead of attempting to fit IoT into existing networks. These approaches are generally solving a solution for a specific sub-set of IoT or exploratory pieces for the usage of new technologies, like the adaptation of two-factor authentication for IIoT EV Vehicles described by Chan & Zhou (Chan & Zhou, 2014) or the usage of blockchain as authentication basis (Hammi et al., 2018). This fractured approach to protocols and IoT security also forces the paradigm of edge computing to become inherently less secure – to be universal, it must support this conglomerate of protocols and security measures. To enable such a chaotic set of features without introducing security flaws is unlikely.

7.1.7 Tangential Security

Tangential security is used here to describe issues that are not direct accounted for but can potentially impact the application of cybersecurity to IoT. There issues are generic issues within the IoT ecosystem, and form part of all considerations. As an example, this 'tangential' security can be exemplified by physical location of IoT devices – a tangential aspect to cybersecurity, as it not a direct technical control, but can vastly impact the required actions for a given IoT device. It will be important to consider not just the technical capabilities when considering network and storage, but also the physical location and interactions that can occur for every IoT device.

7.1.8 Resilience by Design

IoT has some resiliency by design – devices are assumed to be connected to a network intermittently. This intermittent connection is the direct opposite to traditional high availability (HA) and resilience measures, like failover and active-passive backup connections. These HA technologies are not directly compatibly with IoT, and it is unlikely that IoT devices will ever support such active measures for connection resilience, given the hardware and power restrictions. The inclusion of physical linkages to the logical devices creates a complex interdependence between the two. This complexity creates the possibility for cascade failure across two distinct areas – physical and logical (Wang et al., 2019).

7.1.9 Maintenance

The guidance analysed by the research had minimal specific information about maintenance of IoT devices or the potential challenges of maintaining IoT devices and associated systems themselves. Generally, maintenance functions would be implied or required to exist to fulfil other requirements – for example, the ability to remotely update IoT devices implied some sort of maintenance procedure, internal policy, and potentially specific tooling.

This dearth of literature also extends into IoT device-specific maintenance beyond cursory principles and generalisations. IoT lends itself to remote-based maintenance, as physical access to IoT devices can potentially be problematic.

This lack of guidance presents a significant gap in the body of knowledge for IoT maintenance; lacking tried and tested policies and guidelines creates the potential for poor IoT maintenance. Currently, obtaining these specifics requires inference from the characteristics of IoT. Poor maintenance will have a flow-on effect on cybersecurity, given that maintenance should cover the lifetime of a device for updates and upgrades. These specifics will be heavily influenced by an organisation's internal policies and procedures.

7.2 PROCESS CONSIDERATIONS

In addition to technical controls, the processes that govern how an organisation operates must also be considered. These processes are not always solely technical processes – day-to-day operations, like inventory management also affect other operational areas of an organisation, and IoT is not isolated from these adjacent influences. The documents analysed by the research either implied the existence of these related processes, or when they were specifically mentioned, were lacking detail.

7.2.1 Asset Management

The process of asset management is one of the most 'invisible' and one of the longest-running actions that will be undertaken by an organisation – it is continual, ongoing and does not end until the organisation shuts its doors. This often tedious, long-running action runs the risk of being left by the wayside as 'more important' actions occur. Should an undocumented asset appear, all subsequent cybersecurity actions would be compromised, as these protections cannot be applied to an unknown asset.

This catalogue of assets can take different forms, and is not always a single, cohesive system – especially when this catalogue of assets spans multiple systems. As an example, Human Resources systems are unlikely to be integrated into cybersecurity monitoring systems. This split creates potential areas for the overall asset inventory to degrade – be it due to information mismatch, incorrect data entry, administrative neglect or a myriad of other factors that can influence a process. BYOD can compound this possible degradation by adding devices that are not controlled directly by the organisations to their network – if a form of MDM is not used. It's estimated that the number of connected devices will expand to above seven per person ("Global Internet of Things (IoT) Market Growing To Reach on an Average 7 Connected Devices per Person By 2020," 2018). The interruption of Covid19 to office networking has only temporarily ameliorated the coming issue of tracking IoT devices on corporate networks. In a similar vein to BYOD, IoT devices will require additional ruleset and training for employees to be aware of the potential pitfalls of IoT devices when taken into an organisational context.

An example of asset management features in mainstream consumerism can be seen in smartphones and desktop PC's. Specifically, Android smartphones can use the 'Find My Device' functionality – which includes the ability remotely lock, track, and completely wipe a configured device; Apple devices based on iOS have a similar functionality, via the 'Find my iPhone/iPad' equivalent from Apple. In a similar vein, desktops running MacOS or Windows8+ can perform a refresh – reverting all operating system parameters to a fresh install, while leaving users documents and other data alone.

The tracing of assets - their location, current lifecycle state, purpose and overall status is onerous work - leading to the slippage - with typical networks that number potentially hundreds of devices. IoT devices will require even greater detail due to their size, number, and potential geospatial separation.

Generally, ICT based physical identifiers are not as complicated, as each organisation will purchase a unit, and that unit will be marked with a single serial number for the purpose of identification to a manufacturer. However, IoT devices are not always guaranteed to have a physical 'part' of the device that contains the serial number - due to the assumption in the IoT guidance that IoT devices will support secure hardware storage that can contain a unique identifier for that device. This functionality also assumes that this secure hardware storage cannot be altered once the device is received from the manufacturers, and devices will not have a collision of identifiers provisioned in this way.

The format of this serial or identification number has no standard – each manufacturer can implement its own. If an ICT device has more than a single physical identifier – which, if an IoT device is made of multiple devices combined into one (e.g., base device plus a suite of additional sensors) is almost certain to be the case, the cataloguing of these devices would need to take this into account. A modular device without this module-level tracking would run the risk of a devices individual parts being lost or untracked – leading to missing or mismatched devices and parts in the asset management system.

As this asset management system is generally the first source of data for compliance checks and management of existing hardware, any errors in this system would require a physical check of devices. Given the scale of IoT devices and their potential geospatial separation from core offices, this could be costly in both human and financial resources.

Finally, maintenance is a part of the device lifecycle. IoT devices are presumed to have the ability to have most (if not all) maintenance performed remotely – there is no guarantee that a device will support this feature. If a device lacks this functionality, the maintenance would of such device would become a manual process. This process is potentially prohibitive in time and effort due to the compute restrictions of IoT devices, their (usually) small form-factor - which limits the ability to use graphical user interfaces, the potential geospatial separation, and the number of devices.

7.2.2 Disaster Recovery Planning

As IoT can now expand digital commands to physical actions at an ever-increasing scale, business plans must account for this new source of potential risk that IoT can pose – lest the plans contain omissions preventing effective execution and subsequent recovery to normal operations. Chief among these plans will be disaster recovery, especially when the physical actions contain significant potential impact, as would be the case with critical infrastructure services, like water supplies.

In the past, these interactions were restricted to SCADA (Supervisory Control and Data Acquisition) networks. These SCADA networks generally require special hardware and are often air-gapped from other networks due to their nature – there are no easy ways to implement modern security controls on legacy SCADA networks as the protocols and devices were not designed during a time this was thought to be necessary.

As IoT devices make physical interactions more ubiquitous, the assessments for critical infrastructure must include the physical actions that could indirectly affect the operation of the critical asset during a recovery scenario. The expansion in scope to include IoT should be considered when testing the plans, simulating the protected failure of the IoT device to ensure that the physical interactions are as expected.

7.2.3 Policy Creation and Maintenance

Policy guidance is mainly applicable to business, with little to no impact on usage at the consumer level. The policies must not be confused with legal, regulatory requirements as they are only applicable within an organisation. Policies are most effective when they are disseminated, understood, and enforced – if one of these aspects is lacking, the overall effectiveness of any policy across an organisation suffers. Policies are usually used to enforce specific procedures, protections, or provide a strategy to enable desired actions within an organisation.

There is a lack of guidance on what substantiates an ideal cybersecurity policy. There is a sliding scale of view that policies are either principles based, or detailed guidance. While a principles-based approach is lacking in detail, this does not mean that all aspects that are guided by the policy are going to be affected in a negative manner; rigidity in a policy may make cybersecurity more difficult as the mandated procedures have no 'wiggle room' to innovate or pivot directions in response to shifting cybersecurity requirements.

The dissemination of policies also means that they must be understood by a layperson – there are no awards won for the most complicated policies being written, as there is a good chance they will be misinterpreted, misunderstood, or ignored. This means that lines must be toed between creating detailed policies that cover the measurable, strategic goals that want to be achieved and that can be understood by a layperson (Bayuk et al., 2012).

The small amount of guidance presented is principles-based, with the goal of guiding behaviour that will enhance security measures and enabling long-term strategic goals. The base assumption is that policies will already exist and will be expanded or added to implement IoT cybersecurity.

To solve this, the guidance should provide enough information for an organisation to 'come in fresh' and create effective policies that enable the technical guidance provided in the rest of the document, and do not assume that other policies would exist.

7.3 How IoTSOF and IoTSOF-E Fill the Gap

When implementing a framework, the abstracted workflow follows a generic two-step process of selection and then implementation. Generally, the goal of this implementation is to bring about the goal stated by the framework – be that a new process, new procedures, preparation for certification, or new cybersecurity protections.

With each of these two steps, and organisation will undertake a myriad of actions that are abstracted away at this level of generalisation - discussions, analysis and collaborative are just some of the smaller actions that would be needed to occur to implement a new framework across an organisation. However, these actions are external to the analysis of the framework and its effects and are therefore not the focus of the discussion. Figure 33 depicts the theoretical workflow for implementation of a framework focussed on cybersecurity protections – there are no omissions or weaknesses in the framework, and when coupled with an implementation, there are no omissions in the protections applied.

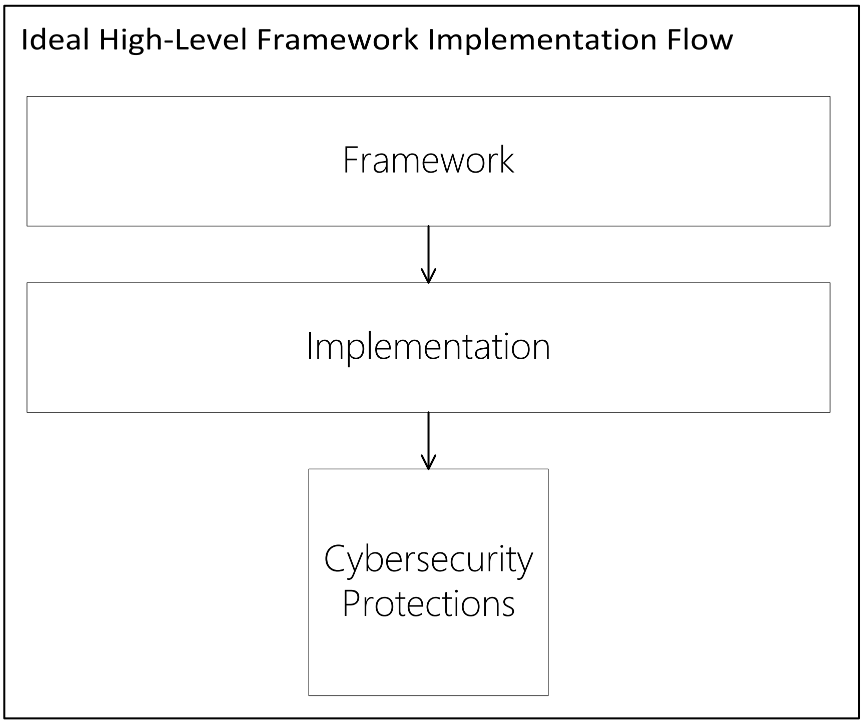

Ideal High-Level Framework Implementation Flow
Framework
Implementation
Cybersecurity Protections

Figure 33: Ideal Framework Implementation

When implementing a framework, no implementation will ever be perfect, and no framework will cover every possible eventuality – this is represented by the gaps at different stages in Figure 34. Due to the evolution of technologies, new or altered approaches, and the continual expansion of knowledge, frameworks are usually long-term, iterative, and collaborative projects. An example of the aforementioned process has produced the Trusted Industry Baseline, which is now at version

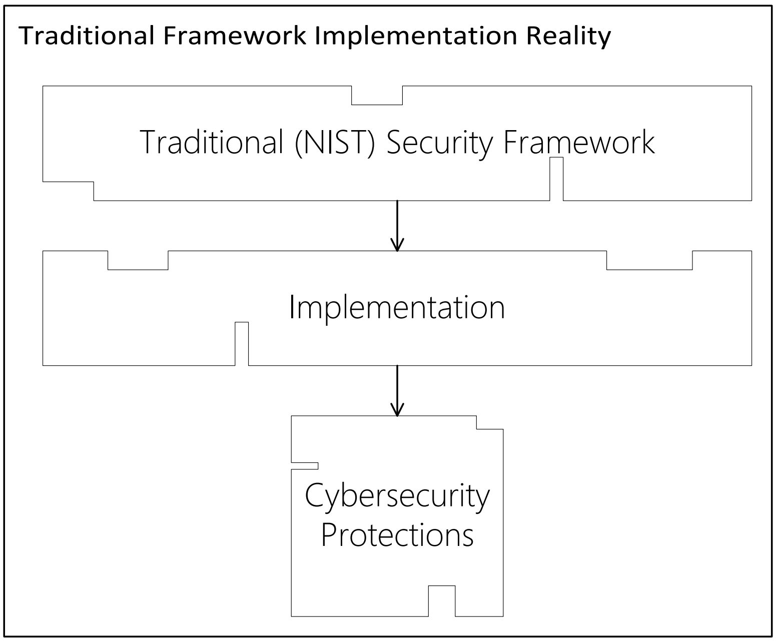

Traditional Framework Implementation Reality
Traditional (NIST) Security Framework
Implementation
Cybersecurity Protections

Figure 34: NIST Framework Implementation

1.1 (National Institute of Standards and Technology, 2018). Despite the robustness of this extensive Trusted Industry Baseline, minor omissions still occur – whether these omissions are due to an imperfect implementation, or an omission from the framework are irrelevant. Ideally, the omissions in a framework are minor enough that accounting for them is trivial when implementing the framework, or the resulting gaps in any cybersecurity protections are small enough to be accepted as an outstanding risk.

In comparison to the smaller number of flaws in the TIB, the analysed IoT guidance contains a greater number of omissions. This increase in omitted content creates an implementation that has more flaws, and the resultant cybersecurity protections due to these larger flaws are more difficult to account for, which is exacerbated by the relative immaturity of administrative tooling for IoT. An example of the flow-on effects these omissions have at the framework level is depicted in Figure 35, with greater gaps present at each stage of the implementation.

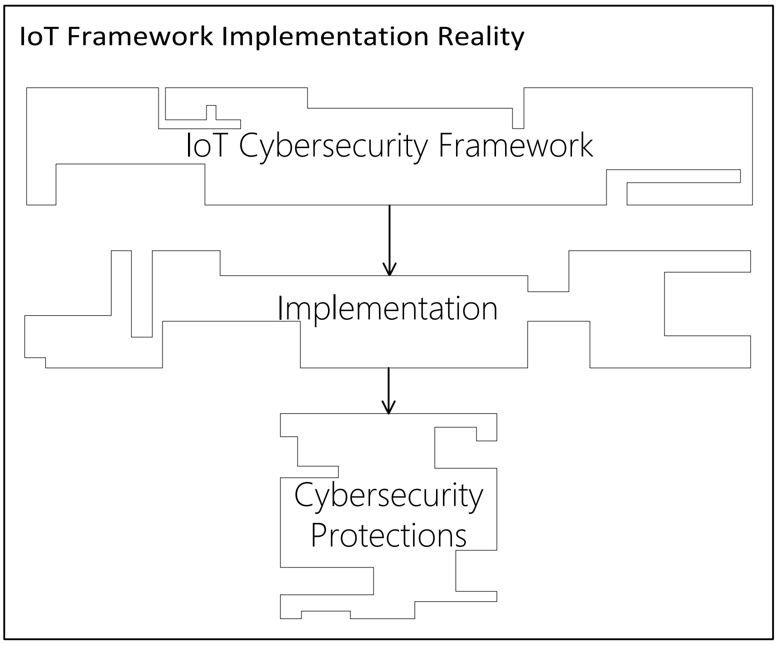

IoT Framework Implementation Reality
IoT Cybersecurity Framework
Implementation
Cybersecurity Protections

Figure 35: IoT Framework Implementation Flow

This research was focussed on applying the already well understood NIST framework to backfill the identified issues in the IoT framework. By doing so, this resulting artifact can be used as overlay against the existing IoT frameworks, compensating for the deficiencies present. This is workflow of overlay and its effect on the resulting cybersecurity protections is shown in Figure 36, with artifact itself located in Appendix A and Appendix B.

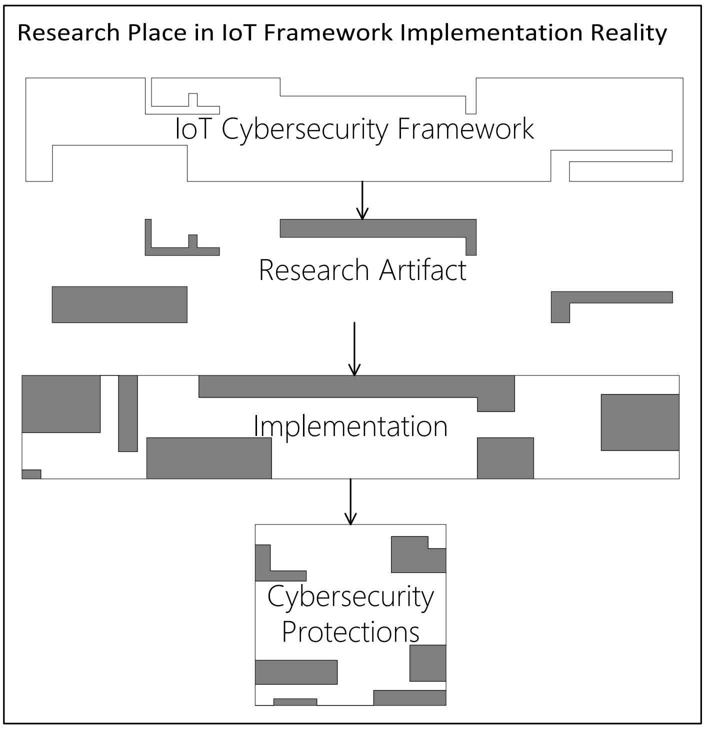

Research Place in IoT Framework Implementation Reality
IoT Cybersecurity Framework
Research Artifact
Implementation
Cybersecurity Protections

Figure 36: Research Artifact Usage

The practical usage of a framework is driven by its perceived usefulness - there is little to no benefit to implementing a flawed framework, as doing so would result in flawed protections. This research allows for the implementation of current frameworks, by addressing the deficiencies that were identified. Additionally, the overlay could be used to generate a new version of the analysed (or a brand new) framework that resolves the identified issues. To demonstrate the variability of the created overlay, a theoretical case and worked example of the framework is demonstrated.

7.4 WORKED EXAMPLE

To demonstrate how to use the framework created by the research, an example case study is used to show the practical application process, by following and expanding the workflow shown in Figure 32 – this expanded workflow is shown in Figure 37.

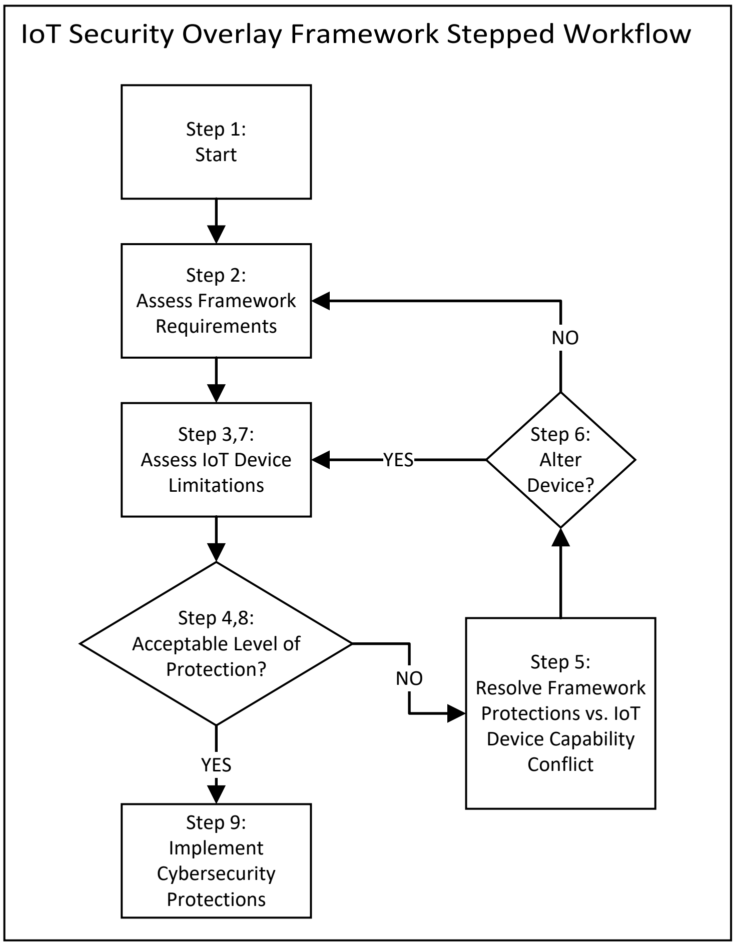

IoT Security Overlay Framework Stepped Workflow
Step 1: Start
Step 2: Assess Framework Requirements
Step 3,7: Assess IoT Device Limitations
Step 4,8: Acceptable Level of Protection?
YES
NO
Step 5: Resolve Framework Protections vs. IoT Device Capability Conflict
Step 6: Alter Device?
YES
NO
Step 9: Implement Cybersecurity Protections

Figure 37: IoT Security Overlay Framework Stepped Workflow

7.4.1 Step One: Start

As shown in Figure 38, the usage of the framework requires some initial groundwork to contextualise the requirements, wants and needs of a given organisation. While the steps in Figure 38 are listed in an order, it is not mandatory that they be completed in this order – just that they are completed. This example will follow the flow from Figure 38.

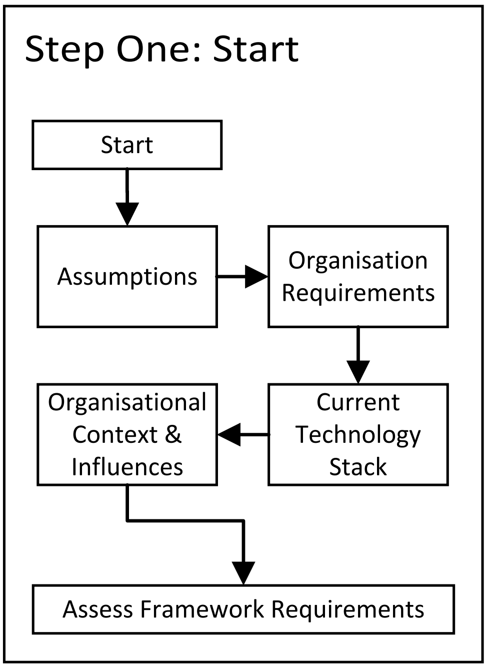

Step One: Start
Start
Assumptions
Organisation Requirements
Current Technology Stack
Organisational Context & Influences
Assess Framework Requirements

Figure 38: IoTSoF Practical Implementation Workflow Expansion: Step One - Start

The following list are the assumptions made for this theoretical implementation.

1. The implementation is fully funded, with no monetary constraints
2. The implementation runs on-time and has a relaxed deadline.
3. The required expertise has been secured externally for the duration of the implementation
4. The current technology stack is known in detail

This set of assumptions moves the process to the next step, organisation requirements. In this step, the exact wants of implementing the framework organisation are articulated. These requirements can be as a simple as desiring 'Better IoT Cybersecurity' or as nebulous and expansive as 'Industry Leading Innovation in IoT Cybersecurity Approaches and effectiveness'. This will vary depending on the assumptions made and the resources an organisation brings to perform the work, and the existing policies, procedures, and approaches already in place. The theoretical organisations requirements are:

1. Both IoTSOF and IoTSOF-E will be implemented
2. The implementation of IoTSOF will enhance the security of our IoT devices and associated networks
    a. This enhanced security will lower our risk of cybersecurity breaches originating from IoT Devices

Having articulated the desired goal, the next step is to map and understand the existing technology stack. Outside of this theoretical example, networks and technologies in an organisation can be far more complex and interrelated. For the example, the following simplified technology stack is presumed to be in use:

1. A monitoring system that can incorporate IoT Devices with multiple identifiers and individual component tracking
2. Existing RBAC
3. Best-Practice PaaS Hybrid-Model Hosting and associated networks

7.4.2 Step Two: Assess Framework Requirements

This worked example only assesses a subsection of the IoTSOF. Specifically, it assesses the code PR.AC – Protection, Access Control, as this subsection demonstrates the full workflow. The detailed workflow for this step is show in Figure 39. Specific actions listed below are taken from the IoTSOF:

1. If centrally managing credentials, ensure devices are integrated into existing access mechanisms
   - Utilise hardware backed secure storage for credentials whenever possible
2. If no hardware secure storage, ensure only administrators have access to credentials
3. Assume that any IoT device in isolated physical locations can be physically tampered with and compromised
4. Prefer devices with either tamper-proof housings or tamper alerts
5. Wherever possible, ensure devices have uniquely bound identities for authentication and authorization

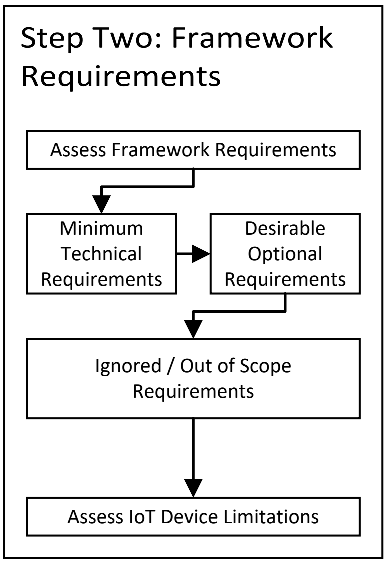

Step Two: Framework Requirements
Assess Framework Requirements
Minimum Technical Requirements
Desirable Optional Requirements
Ignored / Out of Scope Requirements
Assess IoT Device Limitations

Figure 39: IoTSOF Workflow Expansion - Step Two: Framework Requirements

The minimum technical requirements for the organisation in this case is the aim is for best-in-class cybersecurity. This means that the next two steps, desirable-but-optional and out-of-scope requirements are bypassed, and we move the assessment of the IoT device.

7.4.3 Step Three: Assess IoT Device Limitations

The capabilities of a given IoT device will determine the possibility of applying the required protections of the framework. The detailed workflow for this step is shown in Figure 40. For this case, we assume that the device has the following characteristics:

- IoT device does *not* have Crypto Hardware Offload
- Battery powered, intermittent network access
- Still needs secure AuthZ and AuthN, due to data being assessed as requiring protection
- Physical Security measures are possible (Tamper-Proof Housing)

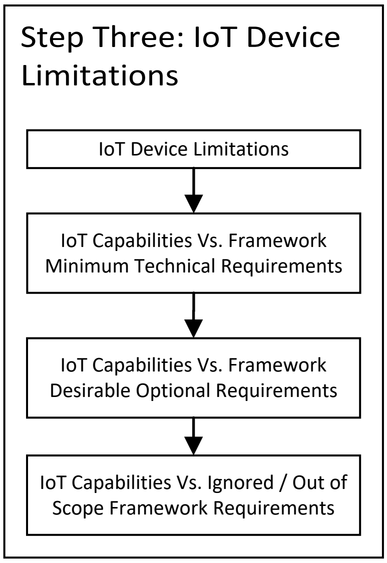

Step Three: IoT Device Limitations
IoT Device Limitations
IoT Capabilities Vs. Framework Minimum Technical Requirements
IoT Capabilities Vs. Framework Desirable Optional Requirements
IoT Capabilities Vs. Ignored / Out of Scope Framework Requirements

Figure 40: Step 3 - IoTSOF Workflow Expansion – Assess IoT Device Limitations

This means that the device in question can be said to have the following capabilities:

- Minimal to no on-board cryptographic capabilities

IoT devices do not usually have the power to spend on cryptographic calculations. Generally, the analysed guidance rejected the usage of software libraries like the OpenSSL project in favour of hardware based cryptographic capabilities.

- Tamper Proof Housing

In this case, the area of deployment for the device is already a secure gated area. This means that while the 'double up' of security measures is the best practice of defence in depth, should the device need to change, the feature of tamper-proof housings or alarms for the IoT device could be dropped if a new device is required.

7.4.3.1 *IoT Device Capabilities vs. Framework Minimum Technical Requirements*

With the limitations of the selected IoT device now known, we can step though the minimum requirements that have been selected by the organisation implementing the framework, discerning if the IoT device will allow for the desired actions to be performed.

The framework actions, as selected in Step 1 are:

- If centrally managing credentials, ensure devices are integrated into existing access mechanisms
  - Utilise hardware backed secure storage for credentials whenever possible

The action to centrally manage the device is potentially a partial pass. The organisation implementing the framework is assumed to have a device management platform that can handle the multiple identifiers that an IoT device may have, passing the initial requirement of being able to manage the devices. However, the IoT device selected currently does not have any dedicated, hardware based cryptographic functions – failing the secondary requirements to use hardware-backed secure storage wherever possible for credentials.

- If no hardware secure storage, ensure only administrators have access to credentials

As the IoT device is assumed to be able to integrate cleaning with the existing device management platform and is most likely running a Unix-like operating system this action is almost certainly technically possible, using the standard Unix permission model.

- Assume that any IoT device in isolated physical locations can be physically tampered with and compromised
  - Prefer device with either tamper-proof housings or tamper alerts

For this deployment of IoT devices in this organisation, the area of deployment is already physically secured. However, applying the principle of defence in depth means that the taper-proof housing and alerting system is still desirable – not only as an additional layer of protection, but in case of deploying the devices outside the physically secure area, providing a measure of physical security built into the device.

- Wherever possible, ensure devices have uniquely bound identities for authentication and authorization

The IoT device and the organisational mobile device management platform is assumed to be able to handle the multiple id's that an IoT device can have. This action is made of multiple technical requirements that must be in sync to ensure the expected functionality. In this case, the IoT device does not have an injected manufacturer identifier, due to it lacking hardware backed secure storage. The device does still have multiple identifiers that can be used to create a unique compound identity for use in the device management system – its MAC address and serial numbers would make an acceptable substitute, with additional generated parameters, like a UUID added as needed. By using the MDM, this can also offload management of AuthZ and AuthN accounts to the MDM, ideally allowing remote update of configuration to all IoT devices.

This explored the technical capabilities of the IoT devices against the selected requirements of the framework. As this theoretical case is aiming for best-in-class cybersecurity protections, there are no 'optional' or 'our of scope' framework actions. At such, we move onto the next step.

7.4.4 Step 4: Acceptable Level of Protection

At this step, a decision must be made against the requirements of the framework against the technical requirements of the device. This must also take into account other operations and a wholistic view of other potential areas of impact.

In this case, the IoT device is lacking hardware based cryptographic functions of any kind. As the data the device is transmitting has been assess as requiring protection, this introduces an overhead to the transmission of the data that renders the function of the device severely degraded – an example of tangential impacts, as this secure data transmission would mainly fall under the purview of 'Protection, Data Security' instead of 'Protection, Authentication'. The requirements for secure data transmission, storage and ongoing cryptographic operations mean that while this 'Protection, Access Control' can technically be performed without the device having this capability of hardware accelerated cryptographic functions, as this is only a smaller step in the organisation implementing the entire framework. At this point, the device now fails the question of 'Do the device, framework and actions combined provide an acceptable level of cybersecurity as defined by the wants and needs of the organisation?

As such, we move on to Step 5 – resolving the conflict to reach an acceptable level of protection.

7.4.5 Step Five: Resolve IoT Device Capabilities vs. Framework Requirements Conflicts

Conflict resolution resolves the differences in requirements of framework vs. the ability of device to fulfill those requirements. This process will result in one of two options being picked. Either the protections that can be put in place are deemed to be sufficient for an organisations' risk appetite after re-assessment, with changes being made to the desired requirements against the framework; or the level of protection is deemed unacceptable, and a different device must be sourced that can meet the requirements. This process will likely result in multiple back-and-forth traversals between device (Step 3) and framework (Step 2) to reach a point where the IoT device and framework are in harmony with the requirements of the organisation.

The framework captures the decision of this confliction resolution by making a binary choice – the change can occur to the IoT device that is going to be implemented, or the change can occur when deciding how to implement that framework. If you reach this point, the implementer has decided that there is a conflict enough to prevent implantation – it must be resolved by altering *something* – it cannot just be ignored. As such, there is no workflow that allows moving from confliction resolution directly to accepting the protections.

For this case, the device lacks a feature that will block other areas of implementation for the framework and severely degrade the functions current section of the framework. As such, we move onto Step 6, whether the device or the framework will be altered to address these shortcomings.

7.4.6 Step 6: Alter Device

As the organisation is aiming for best-in-class IoT cybersecurity, the requirements of the framework cannot be reduced or changed, leaving only the changing of the device as the resolution to this conflict.

In this case, the resolutions to change the device creates the following change to the capabilities of the IoT Device:

- The newly selected IoT device does have hardware cryptographic functions
- The newly selected device drops the tamper-proof housing

As we have made a change to the device, we return to Step 3 – Assess IoT Device limitations. If there were changes to the selected segments of the framework, we would instead return to Step 2 – Assess Framework Requirements.

7.4.7 Step 7: Return to Assess IoT Device Limitations

The new IoT device under assessment has removed one function and added another. As such, only the changed functions need re-assessing. The associated actions of the framework that related to the technical capabilities of the IoT device are:

- Assume that any IoT device in isolated physical locations can be physically tampered with and compromised
    - Prefer device with either tamper-proof housings or tamper alerts

Although the device no longer has a tamper-proof housing or physical access alerting system, the devices are to be deployed in a known secure area – fulfilling the requirement for physical security in a tangential manner, instead of directly by the device. While there is slightly reduced security due to the removal of a layer of security, the requirement still passes due to where the device is deployed. This choice may limit later application of the IoT device to new areas – for example, a non-secure area where the data is still deemed sensitive may present an unacceptable level of protections and risk to the implementer.

- If centrally managing credentials, ensure devices are integrated into existing access mechanisms
    - Utilise secure hardware backed secure storage for credentials whenever possible

The device now supports hardware secure storage and associated cryptographic offload. This impacts the AuthZ and AuthN, by allowing secure storage of credentials, and means that a manufacturer injected unique identifier is likely to be present for usage in the device management system. It also strengthens AuthZ and AuthN, by allowing for more options when selecting the cryptographic implementation.

The rest of the assessment does not change, meaning that we now move onto Step 8, Re-Assessment of Adequate Protection.

7.4.8 Step 8: Re-Assessment of Adequate Protection

As the IoT device now implements hardware cryptographic storage and associated offload, the conflict between IoT device capabilities and Framework Requirements has been resolved. While the loss of the tamper proof housing does result in the loss of a layer of protections, due to the deployment area of a device, this has been deemed an acceptable trade-off.

As such, the selected device and selected framework actions can now be implemented, moving the workflow to Step 9 – Implement Cybersecurity Protections.

7.4.9 Step 9: Implement Cybersecurity Protections

This framework is notably not an implementation guide – as security is a sliding scale based on the unique requirements of each implementation, it would be unfeasible to provide implementation guidance that would suit every department.

Instead, the greater flow of implementation is listed here – that the while the framework is comprised of most atomic actions and is built in a modular fashion, it is best implemented in whole. Figure 41 depicts this overall modular workflow, where each function can be implemented – an implementer may decide to implement a single function (Identify, Protect, Detect, Respond and Recover) (Section 6.2, Table 130) or work through all in order.

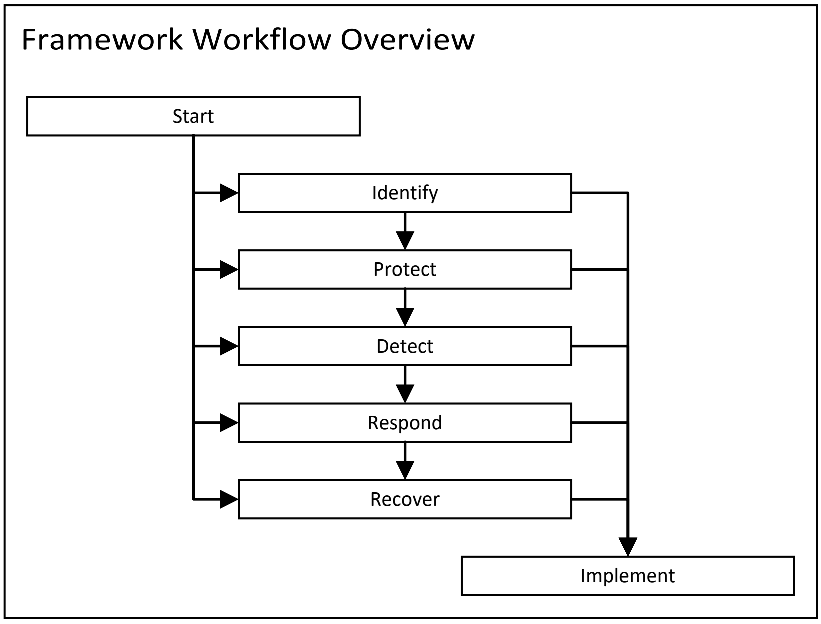


Figure 41: Framework Function Implementation Workflow

As the actions are atomic, each function can be broken down into sub-categories that can be implemented, in whole or in part as well. Each function in Figure 41 is further broken down into its smaller components in Figure 42. Figure 42 show each of the sub-categories from the NIST Document, Section 6.2, Table 130) following the stepped workflow (Figure 37) example for each of the actions specified in the sub-category (Table 130).

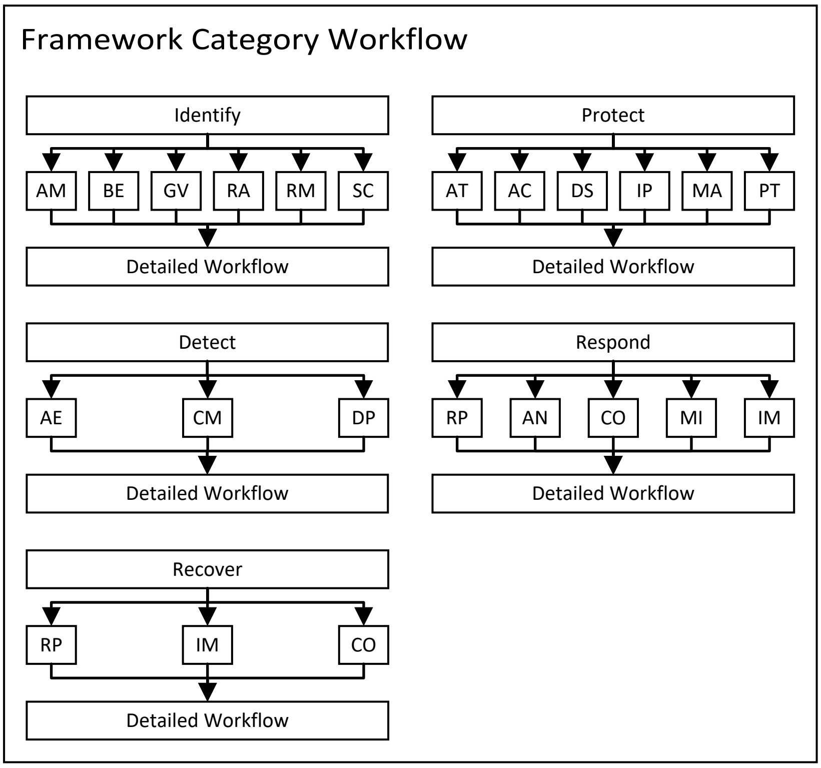


Figure 42: IoTSOF Sub-Category Workflow Components

8 CONCLUSION

This research encompassed and analysed the cybersecurity guidance for IoT, creating a framework to address the shortcomings of existing guidance. This was done using a novel multiple Case Study research approach, allowing the capture of dynamic and context sensitive areas of cybersecurity. Due to the potential proliferation of IoT devices across all aspects of modern digital networks, this research is relevant to implementation and deployment of IoT networks at different scales.

8.1 ANSWERING THE QUESTION

The primary question this research answered is 'How do we create a framework of cybersecurity guidelines to improve the application and effectiveness of cybersecurity for the Internet of Things'. The answer to this question is multifaceted and relied heavily on the research sub-questions to create the building blocks needed. These secondary questions are 'How do we define the Internet of Things (IoT)?' and 'Is it possible to create a categorisation schema for IoT?'.

Firstly, IoT was defined by performing a linguistic analysis of the terminology and language used in the IoT ecosystem. By breaking down the terminology in the IoT Ecosystem and applying a philosophical understanding of the primary linguistic elements leading to a real-world object or logical concept. This follows for individual terms even when the terms appear not to share commonality.

Using this clarification of language along with the ability to map seemingly disparate terms to common approaches or devices, a classification schema for IoT was created. This classification schema moves away from using devices or capabilities as a means to separate devices into categories and is instead focused on where the IoT devices are deployed and the context in which they are used. This categorisation schema is flexible enough to cater to the rapid development of IoT devices while retaining sufficient detail to ensure that different device categories are fit for purpose.

This language analysis and the derived classification schema directly informs the primary research question. Without a clarity of language, you cannot identity IoT devices, or draw any boundaries around the IoT Ecosystem, and thus, cannot apply meaningful cybersecurity protective measures. The classification schema aids in the application of protections, by providing context to the device application – allowing a clear starting point of protection for each category, based on deployment and the data transmitted.

To answer the primary research question "How do we create a framework of cybersecurity guidelines to improve the application and effectiveness of cybersecurity for the 'Internet of Things'", analysis of the existing guidance resulted in the gap-filling framework. This gap-filling framework acts as an overlay to existing guidance, resulting in a new and innovative approach to cybersecurity protections for IoT. Usage of this innovative method does not replace the existing knowledge base of IoT or traditional computing. By contrast, the overlay approach uses synthesis and analysis – thus extracting commonality of cybersecurity guidance from a wide scope of documents to isolate the gaps in existing cybersecurity guidance of IoT. Using these identified gaps resulted in the new overlay frameworks - the Internet of Things Security Overlay Framework (IoTSOF) and the Internet of Things Security Overlay Framework-Ecosystem (IoTSOF-E).

8.2 SIGNIFICANCE

For this research, the significance is made up of the ability to generalise the research to broader applications, and the new approaches to solving identified problems.

8.2.1 Generalising the Research

There are three aspects of this research that can be generalised for broader application. Firstly, the analysis of what is missing from IoT, cross referencing and collating documents can be applied across all areas of research, not just the analysis cybersecurity guidance. To ascertain other area of omissions of the cybersecurity guidance for IoT. The process of taking multiple documents, extracting a common baseline and then analyse for gaps in the document subject is applicable to all case-study based research.

Secondly, the methodological underpinnings of this research are applicable to all case study approaches. By using the methodological approach demonstrated in the research – using multiple cases, each with multiple sub-cases - any research using a case study approach can be enhanced to improve traceability of analysis and conclusions, which are often common criticisms of the case study research method. This is exemplified by the cessation of Cases 2-B, C, D; 3; 4-A, B, C and 5-A, B, C as detailed in Section 5.7 and 5.8, where the modular method (Section 3.3) backed by the methodology of exposure of decision making (Section 3.3.3) allowed the significant deviation of research method without invalidating the overall research methodology.

Finally, the novel method of multi-embedded case studies to target specific contextual views allows the research topics to mirror the system-of-systems under study. This allows investigation of areas of interest for study whilst providing flexibility to account for unexpected discoveries that may change the direction of the research.

8.2.2 The Overlay Approach

Gap filling is a different way of approaching the problem of framework creation. Usually, a framework will be re-written with a new target, when deficiencies are identified, or the target application is different. Instead, this research artifact is designed to be framework agnostic, overlaying the existing work to fill the highlighted gaps. This innovative approach of overlaying on existing work, instead of re-writing, prevents re-work and the creation of new 'ground-up' frameworks that duplicate existing knowledge. By deliberately building on an existing body of knowledge, the effort for a given solution is focused on the new gaps and new issues that need solving - not the already known, effective solutions to existing problems. Nothing currently exists that targets only the gaps in frameworks instead of recreating a framework from scratch. The impact of this is a new approach (gap filling) to the creation and application of cybersecurity frameworks, and the enhancement of existing capabilities.

8.2.3 Common Basis

The analysis of potential sources of IoT cybersecurity guidance and the subsequent tracing of the interrelations between potential documents, revealed a small number of common source documents. This small number was not readily apparent until the complex web of interrelations and cross referencing was traced back to these sources. This set of common references created the possibility to form a common industry baseline. By creating this common baseline, the entire IoT ecosystem is now within scope of analysis, instead of individual documents – allowing greater understanding and effectiveness applying cybersecurity protections for IoT.

This approach of common basis analysis is new to IoT cybersecurity – functioning by taking a holistic approach to existing guidance and identifying the common points of interest for the targeted audiences. Considering contextual nuance is a significant departure from existing analysis approaches, thus creating a brand-new way of looking at an existing body of knowledge. As such, this thesis paves the way for a multitude of new interpretations and applications of this common basis approach to the entirety of Information Technology, not just IoT – in essence, creating an entirely new way to do analysis.

8.2.4 Language

The language surrounding IoT is inconsistent and unhelpful in describing the ecosystem and characteristics of IoT. This is compounded by the complexity of applying cybersecurity to this nascent field of study in which differing perspectives generate new descriptions when describing potential solutions. As discussion in Section 4.5.1, the approach to the analysis of terminology of IoT is the identification of the *components* in a phrase (or acronym), the application of *context* of the interpreter, the identification of the *sense* (loosely, a conceptual understanding) and finally attaching this to a *reference* (the 'real world' object), a novel approach to understanding language in IoT and cybersecurity.

By formulating a common understanding of language for IoT, the need for specialised acronyms can be reduced, if not eliminated. This seemingly simple change has wide-ranging impact for all ICT professionals as it lowers the perceived barrier of language complexity in IoT, hence, the level of specialised knowledge required to perform tasks is reduced. This improved clarity of language also impacts planning, deployments, and implementation – making all three clearer and more independent of hardware and software. This linguistic analysis further enables a way to classify and categorise all new acronyms within the IoT ecosystem – allowing for permanent lexicon to be established regarding the language of IoT that is applicable to any and all people who interact, use, describe or otherwise need to communicate about IoT.

8.2.5 Significance of the IOTSOF/E Framework

When examining the significance of the research, there are multiple degrees of impact that must be considered. We can trace this impact from the community, to the organisation, and to the world.

For this research, the main area of significance is targeting the organisational level. The usage of the research leads to enhanced foundations for the application of cybersecurity protections to IoT – by ensuring more comprehensive framework from which to base implementations from. The better the implementation, the less cybersecurity breaches an organisation can potentially suffer. This overall increase in protection has additional beneficial impacts. There is an improvement in the corporate governance, as implementations of IoT cybersecurity can be better planned, tracked, and have effectiveness related directly to the reduction in IoT based cybersecurity incidents. An organisation can gain financially, as less money is spent on recovery and rectification of damaged systems and consumer reputation. Indeed, reputation can be improved by leading the industry in best practice for IoT cybersecurity. This reputational based trust is critical, as the layperson is now more aware and cares a great deal about known cybersecurity issues – any breaches can be catastrophic to an organisation's reputation.

At a wider scale, worldwide cybersecurity is critical. IoT is prevalent in critical infrastructure, which is one of the first points of attack for the perpetual cyberwarfare. Improved IoT cybersecurity reduces the potential attack surface available to malicious actors, enhancing the security of critical infrastructure.

8.3 Conceptual Significance of the Research

The conceptual significance of the research is different to the generalisability of the research. In this research conceptual significance addresses the requirements of the Shanks' *Theory of Information Systems* (Figure 7), identifying the contributions to scholarship, practical significance, and knowledge.

8.3.1 Contribution to Knowledge

The contribution to knowledge is contained in two aspects of this research – the linguistic analysis and the associated application-based-categorisation schema for IoT together with the IoTSoF/-E framework artifact. The linguistics analysis and breakdown is of particular importance, as it allows for wide understanding of IoT terms that are present now and into the future. The same process can also be applied to other areas of study where language is unclear to increase clarity. Using this clarity, the frameworks specifically add to the body of knowledge surrounding IoT cybersecurity by isolating and identifying the gaps in the current guidance; demonstrates a new way to approach the planning phase of cybersecurity protection at scale by utilising the existing knowledge and then 'gap filling'; and finally creating a new way for these protections to be implemented using the IoTSOF as an overlay to existing protections, instead of constructing a new framework from scratch.

8.3.2 Contribution to Scholarship

One contribution to scholarship is the ability for research to be generalised beyond its initial area. As such, both the methodology and method used in this research is a contribution to scholarship. This consists of an extension to the case study methodology, and a novel way to construct case-studies for the analysis of ICT based systems-of-systems. These components are interlinked – the methodology begins to combat the dearth of instruction on case studies that use multiple cases with multiple topics (Shanks, 2002). Specific note should be drawn to the arguments of rigour of the methodology, the discussion of how rigour can be argued is universal to all case studies.

By using the method to deconstruct an area to be studied into its individual topics, successive cases can be built to examine the detail required. This allows for a dynamic level of investigation as new information comes to light during the research journey. While ideally suited to the changing nature of ICT systems of systems, this method is applicable where there are multiple systems, contextual differences, or continual change within the area of study.

8.3.3 Contribution to Practice

The practical significance of the research focusses on the use of the research outcomes and artifacts. This research is designed to increase cybersecurity protections for any IoT deployment, while limiting the work required by relying on the extensive existing body of knowledge for cybersecurity. The frameworks (IoTSOF/-E) also provide a basis for improvement of existing frameworks, or alternatively, the construction of a new framework to address the shortcomings identified.

The application of a gap-filling framework means that existing known and trusted protections can be left ‘as-is’, preventing the need to recreate or re-certify existing protections that meet the newer requirements mandated by the IoTSOF/E. This reduction in work required allows for greater resources to be focussed on the gaps identified, instead of being ‘wasted’ recreating an existing set of protections.

This novel approach of shortens the time and effort required to iterate when creating, updating, or modifying a cybersecurity implementation - and while the IoTSOF/E is targeted at IoT cybersecurity specifically, the approach itself is generic, and can be applied where there is an existing body of knowledge.

8.4 PERSONAL LEARNINGS

During this research journey, a significant personal learning in the philosophical understanding of the construction of language has been experienced. This language analysis ultimately formed a core portion of the research, however addressing philosophy as a discipline required an unexpectedly different approach and exploration of areas very different to cybersecurity.

This was in addition to the procedural but not less important learning that occurs during a long research journey; learning how to approach research and identifying the deeper meanings behind a given action, reconciling different viewpoints to enable critical analysis across multiple topics and fields of research, collaborating and seeking knowledge from differing sources – these are some of the core foundational skills that have been obtained and polished during the journey of this research.

8.5 Future Research

There are avenues for subsequent research, such as the practical applications and implementation of the IoTSOF/-E or refining the IoTSOF/-E framework with industry.

8.6 Concluding Remarks

This thesis has demonstrated the contextual nuances of cybersecurity when designing protective frameworks for IoT. It has created a baseline security guidance that is applicable to any application of IoT cybersecurity – no matter the scope or complexity of the deployment. By establishing a common understanding of language and canvassing multiple IoT cybersecurity guidance documents to build points of commonality, it has shown that the existing body of knowledge, with some enhancement, can be applied to the newer field of study, namely IoT. This approach to creating a cybersecurity framework as an overlay forms the basis for an entirely new way to think about the creation of cyber protective guidelines and frameworks.

9 REFERENCES

3 billion Yahoo accounts affected in 2013 hack, company says. (2017, October 4). [Text]. ABC News. http://www.abc.net.au/news/2017-10-04/yahoo-says-that-a-2013-breach-affected-all-3-billion/9013502

3GPP. (2021). *Technical Specification Group Services and System Aspects; Catalogue of general security assurance requirements* (Technical Specification (TS) 33.117). 3rd Generation Partnership Project (3GPP). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2440

Abrams, M. D. (2008). *Malicious Control System Cyber Security Attack Case Study–Maroochy Water Services, Australia*. 18.

Abyi, B. R., Minerva; Domenico, Rotondi; (2015). *Towards a Definition of the Internet of Things (IoT)*. http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf

Aced López, S., Corno, F., & De Russis, L. (2015). IoT Meets Caregivers: A Healthcare Support System in Assisted Living Facilities. In R. Giaffreda, R.-L. Vieriu, E. Pasher, G. Bendersky, A. J. Jara, J. J. P. C. Rodrigues, E. Dekel, & B. Mandler (Eds.), *Internet of Things. User-Centric IoT: First International Summit, IoT360 2014, Rome, Italy, October 27-28, 2014, Revised Selected Papers, Part I* (pp. 172–177). Springer International Publishing. https://doi.org/10.1007/978-3-319-19656-5_25

AGELIGHT IoT Safety Architecture & Risk Toolkit (IoTSA) v3.1. (2020). AGELIGHT: AgeLight Digital Trust Advisory Group. https://users.neo.registeredsite.com/9/3/6/20580639/assets/IoTDesignArchitecturev413993.pdf

Ahmed, M., Jaidka, S., & Sarkar, N. I. (2020). Security in Decentralised Computing, IoT and Industrial IoT. In I. Butun (Ed.), *Industrial IoT* (pp. 191–211). Springer International Publishing. https://doi.org/10.1007/978-3-030-42500-5_5

Alder, S. (2021, December 30). Largest Healthcare Data Breaches of 2021. *HIPAA Journal*. https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2021/

Aljabre, A. (2012). *Cloud Computing for Increased Business Value*. *3*(1), 6.

Alnoman, A., & Anpalagan, A. (2017). Towards the fulfillment of 5G network requirements: Technologies and challenges. *Telecommunication Systems*, *65*(1), 101–116. https://doi.org/10.1007/s11235-016-0216-9

Al-Sarawi, S., Anbar, M., Abdullah, R., & Al Hawari, A. B. (2020). Internet of Things Market Analysis Forecasts, 2020–2030. *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, 449–453. https://doi.org/10.1109/WorldS450073.2020.9210375

Alshenqeeti, H. (2014). Interviewing as a Data Collection Method: A Critical Review. *English Linguistics Research*, *3*(1). https://doi.org/10.5430/elr.v3n1p39

Anderson, S., & Williams, T. (2017). Cybersecurity and Medical Devices: Are the ISO/IEC 80001-2-2 Technical Controls up to the Challenge? *Computer Standards & Interfaces*. https://doi.org/10.1016/j.csi.2017.10.001

Arm® Platform Security Architecture Security Model 1.0. (2019). Arm Limited. https://armkeil.blob.core.windows.net/developer/Files/pdf/PlatformSecurityArchitecture/Architect/DEN0079-PSA_SM_ALPHA-02.pdf

ARM Limited, Brightsight B.V, CAICT, Prove & Run S.A.S, Riscure B.V, Trust B.V, & UL TS B.V. (2020). *PSA Certified Level 1 Questionnaire*. https://www.psacertified.org/app/uploads/2020/03/JSADEN001-PSA_Certified_Level_1-2.0-20200210-2.pdf

Article | The Assistance and Access Act: Assisting or Impeding Australia's Tech Industry? | The Legal Forecast. (2019, February 28). http://thelegalforecast.com/article-the-assistance-and-access-act-assisting-or-impeding-australias-tech-industry/

Ashton, K. (2011). That 'internet of things' thing. *RFiD Journal*, *22*(7).

Attaran, M. (2017). The Internet of Things: Limitless Opportunities for Business and Society. *Journal of Strategic Innovation and Sustainability; West Palm Beach*, *12*(1), 10–29.

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

Australian Government. (2014). *Privacy Fact Sheet 17: Australian Privacy Principles*. Office of the Australian Information Commisioner. https://www.oaic.gov.au/resources/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles.pdf

Barker, E., & Roginsky, A. (2019). *Transitioning the use of cryptographic algorithms and key lengths* (NIST SP 800-131Ar2; p. NIST SP 800-131Ar2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-131Ar2

Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures. (2017). European Union Agency For Network And Information Security.

Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012). *Cyber Security Policy Guidebook*. John Wiley & Sons, Incorporated. http://ebookcentral.proquest.com/lib/flinders/detail.action?docID=818205

Belshe, M., Peon, R., & Thomson, M. (2015). *Hypertext Transfer Protocol Version 2 (HTTP/2)* (Request for Comments RFC 7540). Internet Engineering Task Force. https://doi.org/10.17487/RFC7540

Berg, B. L., & Lune, H. (2012). *Qualitative research methods for the social sciences*. Pearson Education.

Berte, D.-R. (2018). Defining the IoT. *Proceedings of the International Conference on Business Excellence*, *12*(1), 118–128. https://doi.org/10.2478/picbe-2018-0013

Bishop, M. (2022). *HTTP/3* (Request for Comments RFC 9114). Internet Engineering Task Force. https://doi.org/10.17487/RFC9114

Boeyen, S., Santesson, S., Polk, T., Housley, R., Farrell, S., & Cooper, D. (2008). *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* (Issue 5280). RFC Editor. https://www.rfc-editor.org/info/rfc5280

Borman, W., Ilgen, D., Klimoski, R., & Weiner, I. (1976). *Handbook of Psychology, Industrial and Organizational Psychology* (Vol. 12). John Wiley and Sons.

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. *Risk Analysis*, *42*(8), 1643–1669. https://doi.org/10.1111/risa.13687

Campbell, D. T., & Stanley, J. C. (2015). *Experimental and quasi-experimental designs for research*. Ravenio Books.

Campbell, S. (2010). Between people and machines. *IEEE Pulse*, *1*(3), 18–25. https://doi.org/10.1109/MPUL.2010.939175

Carroll, N., & Richardson, I. (2016). Software-as-a-Medical Device: Demystifying Connected Health regulations. *Journal of Systems and Information Technology*, *18*(2), 186–215. https://doi.org/10.1108/JSIT-07-2015-0061

Carvalho, M., DeMott, J., Ford, R., & Wheeler, D. A. (2014). Heartbleed 101. *IEEE Security & Privacy*, *12*(4), 63–67. https://doi.org/10.1109/MSP.2014.66

Cassandras, C. G. (2016). Smart Cities as Cyber-Physical Social Systems. *Engineering*, *2*(2), 156–158. https://doi.org/10.1016/J.ENG.2016.02.012

Chan, A. C.-F., & Zhou, J. (2014). Cyber–Physical Device Authentication for the Smart Grid Electric Vehicle Ecosystem. *IEEE Journal on Selected Areas in Communications*, *32*(7), 1509–1517. https://doi.org/10.1109/JSAC.2014.2332121

Checkland, P. (1991). From framework through experience to learning: The essential nature of action research.

Chiuchisan, I., Costin, H. N., & Geman, O. (2014). *Adopting the Internet of Things technologies in health care systems*. 532–535. https://doi.org/10.1109/ICEPE.2014.6969965

Chowdhuryy, M. H. I., & Yao, F. (2021). Leaking Secrets through Modern Branch Predictor in the Speculative World. *IEEE Transactions on Computers*, 1–1. https://doi.org/10.1109/TC.2021.3122830

Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper. (2018). CISCO VNI. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html

Coffey, J. W. (2017). *Ameliorating Sources of Human Error in CyberSecurity: Technological and Human-Centered Approaches*. 4.

Cook, T. D., & Campbell, D. A. (1979). *Quasi-experimental design: Design and analysis issues*. Chicago: Rand McNally.

Cook, T. D., & Campbell, D. T. (1976). *The design and conduct of quasi-experiments and true experiments in fields settings*. Rand McNally.

Cooper, T. (2008). IEC 80001: Proactively managing risks. *24x7 Technology and Service Solutions for Biomeds*.

Cooper, T., & Fuchs, K. (2013). The Wireless Challenge: Technology Risk Assessment In Healthcare Facilities. *Biomedical Instrumentation & Technology*, *47*(3), 202–207. ProQuest Central; ProQuest Medical Library. https://doi.org/10.2345/0899-8205-47.3.202

Council of the European Union. (2016). *EU: General Data Protection Regulation*. http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative and mixed methods approaches* (4th ed.). Sage Publications.

Crozier, R. (2019, March 6). *Australia's anti-encryption laws ridiculed on world stage—Security—ITnews*. https://www.itnews.com.au/news/australias-anti-encryption-laws-ridiculed-on-world-stage-520197

CTIA. (2018). *CTIA Cybersecurity Certification Test Plan for IoT Devices, Version 1.0.1*. CTIA. https://testplansprod.wpengine.com/wp-content/uploads/2019/10/CTIA-IoT-Cybersecurity-Certification-Test-Plan-V1-0-1.pdf

Culpeper, J. (2015). *History of English* (Third Edition). Routledge.

Cybersecurity and Infrastructure Security Agency. (2021, April 8). *Medtronic Conexus Radio Frequency Telemetry Protocol (Update C)*. https://www.cisa.gov/news-events/ics-medical-advisories/icsma-19-080-01

Cyber Security Breaches Survey 2018: Statistical Release. (2018). Department for Digital, Culture, Media and Sport. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf

Dalkey, N., & Helmer, O. (1963). An Experimental Application of the Delphi Method to the Use of Experts. *Management Science*, *9*(3), 458–467. JSTOR. https://doi.org/10.1287/mnsc.9.3.458

Dave, E. (2011). How the next evolution of the internet is changing everything. *The Internet of Things*, 2011.

De Bruin, R., & von Solms, S. H. (2016). Cybersecurity Governance: How can we measure it? *ISTAFRICA*, 1–9. https://doi.org/10.1109/ISTAFRICA.2016.7530578

Dedehayir, O., & Steinert, M. (2016). The hype cycle model: A review and future directions. *Technological Forecasting and Social Change*, *108*, 28–41. https://doi.org/10.1016/j.techfore.2016.04.005

Dhirani, L. L., Armstrong, E., & Newe, T. (2021). Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap. *Sensors*, *21*(11), Article 11. https://doi.org/10.3390/s21113901

Dube, L., & Pare, G. (2003). Rigor in Informations Systems Positivist Case Research: Current Practices, Trends and Recommendations. *MIS Quarterly*, *27*(4), 597–635. ProQuest Central. https://doi.org/10.2307/30036550

Durand, A., Gremaud, P., & Pasquier, J. (2017). Decentralized web of trust and authentication for the internet of things. *Proceedings of the Seventh International Conference on the Internet of Things - IoT '17*, 1–2. https://doi.org/10.1145/3131542.3140263

Eisenhardt, K. M. (1989). Building theories from case study research. (Special Forum on Theory Building). *Academy of Management Review*, *14*(4), 532. https://doi.org/10/ckwzp9

Embedded Hardware Security for IoT Applications (IoTSC-16001; p. 11). (2016). Smart Card Alliance: Internet of Things Security Council. https://www.securetechalliance.org/wp-content/uploads/Embedded-HW-Security-for-IoT-WP-FINAL-December-2016.pdf

European Union & Agency for Network and Information Security. (2017). *Baseline security recommendations for IoT in the context of critical information infrastructures.* http://dx.publications.europa.eu/10.2824/03228

Evans, D. L. (2001). *Security Requirements for Cryptographic Modules* (FIPS 140-2; p. 69). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.FIPS.140-2

Eysenbach, G. (2001). What is e-health? J Med Internet Res, 3(2), e20. https://doi.org/10.2196/jmir.3.2.e20

Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2020). *IoT device cybersecurity capability core baseline* (NIST IR 8259A). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8259a

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival*, *53*(1), 23–40. https://doi.org/10.1080/00396338.2011.555586

Fernandez, F., & Pallis, G. C. (2014). *Opportunities and challenges of the Internet of Things for healthcare: Systems engineering perspective*. 263–266. https://doi.org/10.1109/MOBIHEALTH.2014.7015961

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2020). Teaching and Learning IoT Cybersecurity and Vulnerability Assessment with Shodan through Practical Use Cases. *Sensors*, *20*(11), 3048. https://doi.org/10.3390/s20113048

Fidel, R. (1984). The case study method: A case study. *Library and Information Science Research*, *6*(3), 273–288.

Flavián, C., & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site. *Industrial Management & Data Systems*, *106*(5), 601–620. https://doi-org.ezproxy.flinders.edu.au/10.1108/02635570610666403

Flyvbjerg, B. (2006). Five misunderstandings about case-study research. *Qualitative Inquiry*, *12*(2), 219–245. https://doi.org/Five misunderstandings about case-study research.

Francia III, G., Thornton, D., & Brookshire, T. (2012). Wireless vulnerability of SCADA systems. *Proceedings of the 50th Annual Southeast Regional Conference*, 331–332. https://doi.org/10.1145/2184512.2184590

Frege, G. (1948). Sense and Reference. *The Philosophical Review*, *57*(3), 209. https://doi.org/10.2307/2181485

Gallery, E., & Mitchell, C. J. (2009). Trusted Computing: Security and Applications. *Cryptologia*, *33*(3), 217–245. https://doi.org/10.1080/01611190802231140

Gao, J. C., Liu, J., Rajan, B., Nori, R., Fu, B., Xiao, Y., Liang, W., & Chen, C. L. P. (2014). SCADA communication and security issues. *Security and Communication Networks*, *7*(1), 175–194. https://doi.org/10.1002/sec.698

Geertz, C. (1973). *The interpretation of cultures* (Vol. 5019). Basic books.

Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) (Release 16). (3GPP). https://www.3gpp.org/ftp/Specs/archive/33_series/33.220/

Giaretta, A., Dragoni, N., & Massacci, F. (2019). IoT Security Configurability with Security-by-Contract. *Sensors*, *19*(19), Article 19. https://doi.org/10.3390/s19194121

Gibbert, M., & Ruigrok, W. (2010). The '"What"' and '"How"' of Case Study Rigor: Three Strategies Based on Published Work. *Organizational Research Methods*, *13*(4), 710–737. https://doi.org/10.1177/1094428109351319

Glaser, B. G., & Strauss, A. L. (2017). *Discovery of grounded theory: Strategies for qualitative research*. Routledge.

Global Internet of Things (IoT) Market Growing To Reach on an Average 7 Connected Devices per Person By 2020. (2018, June 25). *M2 Presswire*. http://www.proquest.com/docview/2058426792/citation/B504319756A44843PQ/1

Glotzbach, M. (2009, July 7). *Official Google Blog: Google Apps is out of beta (yes, really)*. https://googleblog.blogspot.com/2009/07/google-apps-is-out-of-beta-yes-really.html

Gluhak, A. V., Ovidiu; Bahr, Roy; Clari, Fabrice; MacchiaMaria, Teresa; Delgado, Teresa; Hoeer, Anne; Bosenberg, Frank; Senigalliesi, Marco; Barchetti, Veronica. (2016). *Report on IoT platform activities* (D03.01). European platforms Initiative. http://www.internet-of-things-research.eu/pdf/D03_01_WP03_H2020_UNIFY-IoT_Final.pdf

Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richer, J. P., Lefkovitz, N. B., Danker, J. M., Choong, Y.-Y., Greene, K. K., & Theofanos, M. F. (2017).

Digital identity guidelines: Authentication and lifecycle management (NIST SP 800-63b). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63b

Greer, C., Burns, M., Wollman, D., & Griffor, E. (2019). *Cyber-physical systems and internet of things* (NIST SP 1900-202). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1900-202

Gruber, B. (2009, August 10). First Wi-Fi pacemaker in US gives patient freedom. *Reuters*. https://www.reuters.com/article/us-pacemaker-idUSTRE5790AK20090810

Guba, E. G., Lincoln, Y. S., & Denzin, N. K. (1994). Handbook of qualitative research. *Califónia: Sage*, 105–117.

Guth, R. A., & Machalaba, D. (2003, August 21). Computer Viruses Disrupt Railroad and Air Traffic. *Wall Street Journal*. https://www.wsj.com/articles/SB106140797740336000

Haghi Kashani, M., Madanipour, M., Nikravan, M., Asghari, P., & Mahdipour, E. (2021). A systematic review of IoT in healthcare: Applications, techniques, and trends. *Journal of Network and Computer Applications*, *192*, 103164. https://doi.org/10.1016/j.jnca.2021.103164

Hajjeh, I., & Badra, M. (2009). *ECDHE_PSK Cipher Suites for Transport Layer Security (TLS)* (Issue 5489). RFC Editor. https://www.rfc-editor.org/info/rfc5489

Hammi, M. T., Hammi, B., Bellot, P., & Serhrouchni, A. (2018). Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Computers & Security*, *78*, 126–142. https://doi.org/10.1016/j.cose.2018.06.004

Hans. (2010, June 15). *IoBridge Tide Alerts on MIT's Technology Review Blog*. IoBridge Blog. http://blog.iobridge.com/2010/06/iobridge-tide-alerts-on-mits-technology-review-blog/

Hardy, Q. (2014, March 27). Consortium Wants Standards for "Internet of Things." *Bits Blog*. https://bits.blogs.nytimes.com/2014/03/27/consortium-wants-standards-for-internet-of-things/

Harris, B., & Hunt, R. (1999). TCP/IP security threats and attack methods. Computer Communications, 22(10), 885–897. https://doi.org/10.1016/S0140-3664(99)00064-X

Health Information Privacy. (2015, August 26). [Text]. HHS.Gov. https://www.hhs.gov/hipaa/index.html

He, D., Chan, S., & Guizani, M. (2017). Cyber Security Analysis and Protection of Wireless Sensor Networks for Smart Grid Monitoring. IEEE Wireless Communications, 24(6), 98–103. https://doi.org/10.1109/MWC.2017.1600283WC

Henton, D., & Held, K. (2013). The dynamics of Silicon Valley: Creative destruction and the evolution of the innovation habitat. *Social Science Information*, *52*(4), 539–557. https://doi.org/10.1177/0539018413497542

Hevner, A., & Chatterjee, S. (2010). *Design Research in Information Systems* (Vol. 22). Springer US. https://doi.org/10.1007/978-1-4419-5653-8

HIPAA: Security Checklist. (2019). HipaaOne. https://www.hipaaone.com/wp-content/uploads/2019/01/HIPAA-Security-Checklist-1-10-2019.pdf

Hiral B. Patel, Nirali Kansara, *Cloud Computing Deployment Models: A Comparative Study*, International Journal of Innovative Research in Computer Science & Technology **(IJIRCST),** 2021, 9(2), PP45-50

Hofseth, L. J. (2018). Getting rigorous with scientific rigor. *Carcinogenesis*, *39*(1), 21–25. PubMed. https://doi.org/10.1093/carcin/bgx085

Honan, R., Lewis, T. W., Anderson, S., & Cooke, J. (2020). A Quantum Computer Operating System. In M. Qiu (Ed.), *Algorithms and Architectures for Parallel Processing* (pp. 415–431). Springer International Publishing.

Identity and Access Management for the Internet of Things—Summary Guidance. (2016). Cloud Security Alliance (CSA). https://cloudsecurityalliance.org/artifacts/identity-and-access-management-for-the-iot/

Igure, V. M., Laughter, S. A., & Williams, R. D. (2006). Security issues in SCADA networks. Computers & Security, 25(7), 498–506. https://doi.org/10.1016/j.cose.2006.03.001

International Electrotechnical Commission. (2009). *Industrial communication networks—Network and system security—Part 1-1: Terminology, concepts and models* (IEC TS 62443-1-1). https://webstore.iec.ch/publication/7029

International Electrotechnical Commission. (2009). *Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components* (IEC 62443-4-2). https://webstore.iec.ch/publication/34421

International Organization for Standardization. (2019). *Environmental management systems—Guidelines for a flexible approach to phased implementation* (ISO 14005:2019). https://www.iso.org/obp/ui/#iso:std:iso:14005:ed-2:v1:en

International Organization for Standardization, International Electrotechnical Commission. (2013).

Information technology—Security techniques—Information security management systems—Requirements (ISO/IEC 27001:2013). https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

International Organization for Standardization, International Electrotechnical Commission. (2018). *Information technology—Open Connectivity Foundation (OCF) Specification—Part 1: Core specification* (ISO/IEC 30118-1:2018). https://www.iso.org/obp/ui/#iso:std:iso-iec:30118:-1:ed-1:v1:en

Internet Census 2012. (2015, October 13). https://web.archive.org/web/20151013010243/http://internetcensus2012.bitbucket.org/paper.html

Internet of Things (IoT). (2017). https://www.intel.com/content/www/us/en/internet-of-things/overview.html

Internet of Things (IoT) Market (2021-26) | Industry Size, Growth, Trends. (2020). Mordor Intelligence. https://www.mordorintelligence.com/industry-reports/internet-of-things-moving-towards-a-smarter-tomorrow-market-industry

Internet of Things (IoT) Security and Privacy Recommendations. (2016a). Broadband Internet Technical Advisory Group. https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

Internet of Things (IoT) Security and Privacy Recommendations. (2016b). BITAG. https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

Internet of Things (IoT) security best practices | Microsoft Docs. (2018, October 9). https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices

Internet of Things: Privacy & Security in a Connected World (p. 71). (2015). Federal Trade Commission. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

Internet of Things Security Foundation: IoT Security Compliance Framework. (2016). IoT Security Foundation. https://iotsecurityfoundation.org/wp-content/uploads/2016/12/IoT-Security-Compliance-Framework.pdf

IoT Alliance Australia: Internet of Things Security Guidelines. (2017). http://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf

IoT Framework Assessment—OWASP. (2016, May 14). https://www.owasp.org/index.php/IoT_Framework_Assessment

IoT Security & Privacy Trust Framework v2.5. (2017). Online Trust Alliance (OTA). https://www.internetsociety.org/resources/doc/2018/iot-trust-framework-v2-5/

Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The Internet of Things for Health Care: A Comprehensive Survey. *Ieee Access*, *3*, 678–708. https://doi.org/10.1109/Access.2015.2437951

ITU Internet Report, 2005: The Internet of Things, Executive Summary (p. 28). (2005). International Telecommunications Union. http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf

Jick, T. D. (1979). Mixing qualitative and quantitative methods: Triangulation in action. *Administrative Science Quarterly*, *24*(4), 602–611. https://doi.org/10/dd4b5d

Johnson, R. B., Onwuegbuzie, A. J., & Turner, L. A. (2007). Toward a Definition of Mixed Methods Research. *Journal of Mixed Methods Research*, *1*(2), 112–133. https://doi.org/10.1177/1558689806298224

Joint Task Force Transformation Initiative. (2013). *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST SP 800-53r4). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r4

Kandhari, K. (2014, September 25). "Bend-Gate": An Apple iPhone 6 Plus Feature That Is Troubling Users. *EFYTimes.Com*. http://www.proquest.com/docview/1564595217/abstract/ED624ABB4BDE408BPQ/1

Kasprzak, S. (2017). Samsung: Batteries Caused Galaxy Note7 Fires, Expands Recall. *Product Design & Development*. http://www.proquest.com/docview/1861049067/citation/856E4D0E84FA4217PQ/1

H.R.1668—IoT Cybersecurity Improvement Act of 2020, H.R.1668, Congress, 116 (2020). http://www.congress.gov/

Kemmerer, R. A. (2003). Cybersecurity. *25th International Conference on Software Engineering, 2003. Proceedings.*, 705–715. https://doi.org/10.1109/ICSE.2003.1201257

Khan, A. W., Zaib, S., Khan, F., Tarimer, I., Seo, J. T., & Shin, J. (2022). Analyzing and Evaluating Critical Cyber Security Challenges Faced by Vendor Organizations in Software Development: SLR Based Approach. *IEEE Access*, 1–1. https://doi.org/10.1109/ACCESS.2022.3179822

Khan, Z., Anjum, A., Soomro, K., & Tahir, M. A. (2015). Towards cloud based big data analytics for smart future cities. *Journal of Cloud Computing*, *4*(1). https://doi.org/10.1186/s13677-015-0026-8

Kidder, L. H. (1986). *Research methods in social relations* (5th ed.). New York : Holt, Rinehart and Winston.

Kindervag, J., & Balaouras, S. (2010). No More Chewy Centers: Introducing The Zero Trust Model Of Information Security. *Forrester Research*, *3*, 15.

Kirk, J., & MIller, M. L. (1986). *Reliability and Validity in Qualitative Research* (Vol. 1). United States of America, California, Newbury Park: SAGE Publications, Inc. https://doi.org/10.4135/9781412985659

Klein, S. R., & Monson, R. A. (2015). *Beyond HIPAA: Connected Health Care and the Internet of Things*.

Kobara, K. (2016). Cyber Physical Security for Industrial Control Systems and IoT. IEICE Transactions on Information and Systems, E99.D(4), 787–795. https://doi.org/10.1587/transinf.2015ICI0001

Kuzin, M., Shmelev, Y., & Kuskov, V. (2018, September 18). *New trends in the world of IoT threats*. https://securelist.com/new-trends-in-the-world-of-iot-threats/87991/

Kvale, S. (1996). *InterViews: An introduction to qualitative reserach interviewing.* Sage Publications.

Kvedar, J. C. (2016). *Harnessing the Internet of Healthy Things*. Partners Connected Health. http://www.himssasiapac.org/sites/default/files/HIMSSAP_ThematicReport_HarnessingtheInternetofHealthThings.pdf

Labott, E. (2003, September 24). *Welchia worm hits U.S. State Dept. Network*. http://edition.cnn.com/2003/TECH/internet/09/24/state.dept.virus/index.html

Layden, J. (2008, January 11). Polish teen derails tram after hacking train network. *The Register*. https://www.theregister.co.uk/2008/01/11/tram_hack/

Lee, A. S., & Baskerville, R. L. (2003). Generalizing generalizability in information systems research. *Information Systems Research*, *14*(3), 221–243. https://doi.org/10/bn3mff

Lee, E.-K., Lim, J.-H., & Kim, J. (2017). Prioritized access control enabling weighted, fine-grained protection in cyber-physical systems. *International Journal of Distributed Sensor Networks*, *13*(12), 155014771774890. https://doi.org/10.1177/1550147717748908

Levi, M., Allouche, Y., & Kontorovich, A. (2018). Advanced Analytics for Connected Car Cybersecurity. *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, 1–7. https://doi.org/10.1109/VTCSpring.2018.8417690

Lipner, S. (2004). The Trustworthy Computing Security Development Lifecycle. 20th Annual Computer Security Applications Conference, 2–13. https://doi.org/10.1109/CSAC.2004.41

Lipp, M., Schwarz, M., Gruss, D., Prescher, T., Haas, W., Mangard, S., Kocher, P., Genkin, D., Yarom, Y., & Hamburg, M. (2018). *Meltdown* (arXiv:1801.01207). arXiv. http://arxiv.org/abs/1801.01207

Lopez, J., & Wu, Y. (Eds.). (2015). Information Security Practice and Experience: 11th International Conference, ISPEC 2015, Beijing, China, May 5-8, 2015, Proceedings (Vol. 9065). Springer International Publishing. https://doi.org/10.1007/978-3-319-17533-1

Ludvigsen, K., Nagaraja, S., & Daly, A. (2022). When Is Software a Medical Device? Understanding and Determining the "Intention" and Requirements for Software as a Medical Device in European Union Law. *European Journal of Risk Regulation*, *13*(1), 78–93. https://doi.org/10.1017/err.2021.45

Lv, Z., Qiao, L., Verma, S., & Kavita. (2021). AI-enabled IoT-Edge Data Analytics for Connected Living. *ACM Transactions on Internet Technology*, *21*(4), 1–20. https://doi.org/10.1145/3421510

Lyytinen, K., & Yoo, Y. (2002). Ubiquitous computing. *Communications of the ACM*, *45*(12), 63–96.

Maoz, Z. (2002). Case study methodology in international studies: From storytelling to hypothesis testing. *Evaluating Methodology in International Studies: Millennial Reflections on International Studies*, 161–186.

Mark Schildhauer, M. B. J. (2016). *OBOE: The Extensible Observation Ontology, version 1.1*. KNB Data Repository. https://doi.org/10.5063/F11C1TTM

Martin, A. (2014). *Corporate response to bring your own device (BYOD)* [M.S., Utica College]. https://www.proquest.com/docview/1535294310/abstract/BED44F7AF4A84276PQ/1

Master IoT Cyber-Security Challenges with Comprehensive, Multi-layer Security: Larger attack surface, outdated hardware, weak credentials and lack of accountability among IoT cyber-security challenges--in a new article from eMazzanti Technologies. (2019, September 19). *PR Newswire*. https://www.proquest.com/docview/2292886034/citation/1A4E6D6FD55A460CPQ/1

McCue, T. J. (2015, April 22). *$117 Billion Market For Internet of Things In Healthcare By 2020*. Forbes. https://www.forbes.com/sites/tjmccue/2015/04/22/117-billion-market-for-internet-of-things-in-healthcare-by-2020/

McElroy, D. (2012, May 28). *Flame: World's most complex computer virus exposed*. https://www.telegraph.co.uk/news/worldnews/middleeast/iran/9295938/Flame-worlds-most-complex-computer-virus-exposed.html

McGaghie, W. C., Bordage, G., & Shea, J. A. (2001). Problem Statement, Conceptual Framework, and Research Question. *Academic Medicine*, *76*(9), 923. https://doi.org/10.1097/00001888-200109000-00021

McGinn, C. (2015). *Philosophy of Language: The Classics Explained*. MIT Press. http://ebookcentral.proquest.com/lib/flinders/detail.action?docID=3339941

McGrew, D., & Bailey, D. (2012). *AES-CCM Cipher Suites for Transport Layer Security (TLS)* (Issue 6655). RFC Editor. https://www.rfc-editor.org/info/rfc6655

McMillan, R. (2006, October 31). *Hackers break into water system network*. Computerworld. https://www.computerworld.com/article/2547938/hackers-break-into-water-system-network.html

Merriam-Webster. (n.d.). Internet of Things. In *Merriam-Webster.com dictionary*. Retrieved June 21, 2020, from https://www.merriam-webster.com/dictionary/Internet+of+Things

Mhaskar, N., Alabbad, M., & Khedri, R. (2021). A Formal Approach to Network Segmentation. Computers & Security, 103, 102162. https://doi.org/10.1016/j.cose.2020.102162

Michler, O., Decker, R., & Stummer, C. (2020). To trust or not to trust smart consumer products: A literature review of trust-building factors. *Management Review Quarterly*, *70*(3), 391–420. https://doi.org/10.1007/s11301-019-00171-8

Mineraud, J., Mazhelis, O., Su, X., & Tarkoma, S. (2016). A gap analysis of Internet-of-Things platforms. *Computer Communications*, *89–90*, 5–16. https://doi.org/10.1016/j.comcom.2016.03.015

Miranda, J., Cabral, J., Wagner, S. R., Fischer Pedersen, C., Ravelo, B., Memon, M., & Mathiesen, M. (2016). An Open Platform for Seamless Sensor Support in Healthcare for the Internet of Things. *Sensors (Basel)*, *16*(12), 2089. https://doi.org/10.3390/s16122089

Moeller, B., Bolyard, N., Gupta, V., Blake-Wilson, S., & Hawk, C. (2006). *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)* (Issue 4492). RFC Editor. https://www.rfc-editor.org/info/rfc4492

Moore, G. E. (1998). Cramming More Components onto Integrated Circuits. *PROCEEDINGS OF THE IEEE*, *86*(1), 4.

Munro, K. (2008). SCADA–A critical situation. *Network Security*, *2008*(1), 4–6. https://doi.org/10.1016/S1353-4858(08)70005-9

National Institutes of Health. (2015, August 13). *Principles and Guidelines for Reporting Preclinical Research*. National Institutes of Health (NIH). U.S. Department of Health and Human Services. https://www.nih.gov/research-training/rigor-reproducibility/principles-guidelines-reporting-preclinical-research

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (NIST CSWP 04162018; p. NIST CSWP 04162018). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

National Institute of Standards and Technology. (2019). *Security requirements for cryptographic modules* (NIST FIPS 140-3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.FIPS.140-3

NEMA. (2018). *Cyber Hygiene Best Practices*. National Electrical Manufacturers Association (NEMA). https://www.nema.org/Standards/Pages/Cyber-Hygiene-Best-Practices.aspx

Nguyen, K. T., Laurent, M., & Oualha, N. (2015). Survey on secure communication protocols for the Internet of Things. *Ad Hoc Networks*, *32*, 17–31. https://doi.org/10.1016/j.adhoc.2015.01.006

Noca, M. (2009). *Swiss Cube | The first swiss satellite*. http://swisscube.epfl.ch/

Numagami, T. (1998). Perspective—The infeasibility of invariant laws in management studies: A reflective dialogue in defense of case studies. *Organization Science*, *9*(1), 1–15. https://doi.org/10/cjkd6t

Nurse, J. R. C., Creese, S., & De Roure, D. (2017). Security Risk Assessment in Internet of Things Systems. *IT Professional*, *19*(5), 20–26. https://doi.org/10.1109/MITP.2017.3680959

OCF Security Specification Version 2.1.2. (2020). Open Connectivity Foundation.

Official Document CLP.11 – IoT Security Guidelines Overview Document Version 2.0. (2017). GSM Association. https://www.gsma.com/iot/gsma-iot-security-guidelines-complete-document-set/

Official Document CLP.12—IoT Security Guidelines for IoT Service Ecosystem Version 2.0. (2017). GSM Association. https://www.gsma.com/iot/gsma-iot-security-guidelines-complete-document-set/

Official Document CLP.13—IoT Security Guidelines Endpoint Ecosystem Version 2.0. (2017). GSM Association. https://www.gsma.com/iot/gsma-iot-security-guidelines-complete-document-set/

Official Document CLP.14—IoT Security Guidelines for Network Operators Version 2.0. (2017). GSM Association. https://www.gsma.com/iot/gsma-iot-security-guidelines-complete-document-set/

O'Leary, D. E. (2008). Gartner's hype cycle and information system research issues. *International Journal of Accounting Information Systems*, *9*(4), 240–252. https://doi.org/10.1016/j.accinf.2008.09.001

Palanisamy, R., Norman, A. A., & Mat Kiah, L. (2021). BYOD Security Risks and Mitigation Strategies: Insights from IT Security Experts. *Journal of Organizational Computing and Electronic Commerce*, *31*(4), 320–342. https://doi.org/10.1080/10919392.2022.2028530

Pandey, R., Paprzycki, M., Srivastava, N., Bhalla, S., & Wasielewska-Michniewska, K. (Eds.). (2021). *Semantic IoT: Theory and Applications: Interoperability, Provenance and Beyond* (Vol. 941). Springer International Publishing. https://doi.org/10.1007/978-3-030-64619-6

Pasha, M., & Shah, S. M. W. (2018). Framework for E-Health Systems in IoT-Based Environments. *Wireless Communications and Mobile Computing*, *2018*, 1–11. https://doi.org/10.1155/2018/6183732

Patil, R. A., & Ramakrishna, S. (2020). A comprehensive analysis of e-waste legislation worldwide. *Environmental Science and Pollution Research*, *27*(13), 14412–14431. https://doi.org/10.1007/s11356-020-07992-1

Pettigrew, A. M. (1990). Longitudinal field research on change: Theory and practice. *Organization Science*, *1*(3), 267–292. https://doi.org/10/b57nfx

Plummer, D. C., Bittman, T. J., Austin, T., Cearley, D. W., & Smith, D. M. (2008). *Cloud Computing: Defining and Describing an Emerging Phenomenon*. 9.

Postscapes. (2019, January 11). '*Tracking the Internet of Things*' [Postscapes IoT Protocol Overview]. Postscapes. https://www.postscapes.com/wp-content/uploads/2018/03/connectivity-diagram-768x449.jpg

Popper, K. (2005). *The logic of scientific discovery*. Routledge.

Poulsen, K. (2003, August 19). *Slammer worm crashed Ohio nuke plant network*. https://www.securityfocus.com/news/6767/

Proofpoint Uncovers Internet of Things (IoT) Cyberattack. (2014, December 1). https://www.proofpoint.com/us/proofpoint-uncovers-internet-things-iot-cyberattack

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, (2020). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN

PwC. (2017). *Monetizing the industrial Internet of Things* (p. 19). Price Waterhouse Coopers. https://www.pwc.com/us/en/industrial-products/publications/assets/pwc-monetizing-the-industrial-internet-of-things.pdf

Qadeer, A., Waqar Malik, A., Ur Rahman, A., Mian Muhammad, H., & Ahmad, A. (2020). Virtual Infrastructure Orchestration For Cloud Service Deployment. *The Computer Journal*, *63*(2), 295–307. https://doi.org/10.1093/comjnl/bxz125

Qadri, Y. A., Nauman, A., Zikria, Y. B., Vasilakos, A. V., & Kim, S. W. (2020). The Future of Healthcare Internet of Things: A Survey of Emerging Technologies. IEEE Communications Surveys & Tutorials, 22(2), 1121–1167. https://doi.org/10.1109/COMST.2020.2973314

Radanliev, P., De Roure, D. C., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S., & Burnap, P. (2018). Future developments in cyber risk assessment for the internet of things. *Computers in Industry*, *102*, 14–22. https://doi.org/10.1016/j.compind.2018.08.002

Rahman, A., Mahdavi-Hezaveh, R., & Williams, L. (2019). A systematic mapping study of infrastructure as code research. *Information and Software Technology*, *108*, 65–77. https://doi.org/10.1016/j.infsof.2018.12.004

Rahmani, A. M., Gia, T. N., Negash, B., Anzanpour, A., Azimi, I., Jiang, M., & Liljeberg, P. (2018). Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. *Future Generation Computer Systems*, *78*, 641–658. https://doi.org/10.1016/j.future.2017.02.014

Rajkumar, R. (Raj), Lee, I., Sha, L., & Stankovic, J. (2010). Cyber-physical Systems: The Next Computing Revolution. *Proceedings of the 47th Design Automation Conference*, 731–736. https://doi.org/10.1145/1837274.1837461

Rani, D., & Gill, N. S. (2019). *Review of Various IoT Standards and Communication Protocols*. *12*(5), 11.

Ravitch, S. M. (2017). *Reason & rigor: How conceptual frameworks guide research* (Second Edition.). Los Angeles : SAGE.

Ren, J., Guo, H., Xu, C., & Zhang, Y. (2017). Serving at the Edge: A Scalable IoT Architecture Based on Transparent Computing. *IEEE Network*, *31*(5), 96–105. https://doi.org/10.1109/MNET.2017.1700030

Robert, P. F. (2005, August 18). *Zotob, PnP Worms Slam 13 Daimler-Chrysler Plants*. EWEEK. https://www.eweek.com/security/zotob-pnp-worms-slam-13-daimlerchrysler-plants

Rogers, R. H. (2016). Using Lenses to Make Sense of Research: A Review of Sharon M. Ravitch and Matthew Riggan's Reason & Rigor: How Conceptual Frameworks Guide Research. *The Qualitative Report; Fort Lauderdale*, *21*(9), 1708–1712.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, tyw001. https://doi.org/10.1093/cybsec/tyw001

Russell, B., & Duren, D. V. (2016). *Practical Internet of things security: A practical, indispensable security guide that will navigate you through the complex realm of securely building and deploying systems in our IoT-connected world*. Packt Pub.

Sadeghi, A.-R., Wachsmann, C., & Waidner, M. (2015). *Security and privacy challenges in industrial internet of things*. 1–6. https://doi.org/10.1145/2744769.2747942

Salem, S. (2016, February 2). *Key Trends, Opportunities, and Challenges in Healthcare IoT Adoption*. https://iot.knowledge-bytes.com/sites/iot/files/Key-Trends-Opportunities-and-Challenges-in-Healthcare-IoT-Adoption.pdf

Savolainen, R. (1996). The art of case study research: Stake, Robert E. Thousand Oaks, CA: Sage Publications, 1995. 175 pp. $23.50 (paperback). (ISBN 0-8039-5767-X). *Library and Information Science Research*, *18*(3), 291–293. https://doi.org/10/ctgn2w

Scholz, R. W., & Tietje, Olaf. (2002). *Embedded case study methods: Integrating quantitative and qualitative knowledge*. Sage Publications.

Schrecker, S., Soroush, H., Molina, J., Caldwell, J., Meltzer, D., Hirsch, F., Leblanc, J. P., & Buchheit, M. (2016). Industrial internet of things volume G4: security framework. *Ind. Internet Consort*, 1-173.

Serral, E., Stede, C. V., & Hasic, F. (2020). Leveraging IoT in Retail Industry: A Maturity Model. 2020 IEEE 22nd Conference on Business Informatics (CBI), 114–123. https://doi.org/10.1109/CBI49978.2020.00020

Shah, S. H., & Yaqoob, I. (2016). A survey: Internet of Things (IOT) technologies, applications and challenges. *2016 IEEE Smart Energy Grid Engineering (SEGE)*, 381–385. https://doi.org/10.1109/SEGE.2016.7589556

Shanks, G. (2002). Guidelines for Conducting Positivist Case Study Research in Information Systems. Australasian Journal of Information Systems, 10(1), Article 1. https://doi.org/10.3127/ajis.v10i1.448

Shanks, Graeme., Arnott, D., & Rouse, A. (1993). *A review of approaches to research and scholarship in information systems*. Dept. of Information Systems, Faculty of Computing and Information Technology, Monash University; /z-wcorg/.

Sharda, S., Singh, M., & Sharma, K. (2021). Demand side management through load shifting in IoT based HEMS: Overview, challenges and opportunities. *Sustainable Cities and Society*, *65*, 102517. https://doi.org/10.1016/j.scs.2020.102517

Shuaib, M., Samad, A., Alam, S., & Siddiqui, S. T. (2019). Why Adopting Cloud Is Still a Challenge?—A Review on Issues and Challenges for Cloud Migration in Organizations. In Y.-C. Hu, S. Tiwari, K. K. Mishra, & M. C. Trivedi (Eds.), *Ambient Communications and Computer Systems* (pp. 387–399). Springer Singapore.

Silverman, D. (2005). *Doing qualitative research: A practical handbook* (2nd ed.). London : SAGE.

Silverman, D. (2006). *Interpreting qualitative data: Methods for analyzing talk, text and interaction* (3rd ed.). SAGE.

Simoes, P., Cruz, T., Proença, J., & Monteiro, E. (2013, July 11). *On the use of Honeypots for Detecting Cyber Attacks on Industrial Control Networks*. European Conference on Information Warfare and Security, ECCWS.

Skuce, D. (1995). *Conventions for reaching agreement on shared ontologies*. Proceedings of the 9th Knowledge Acquisition for Knowledge Based Systems Workshop.

Smith, T. (2001, October 31). *Hacker jailed for revenge sewage attacks*. https://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/

Soltys, M. (2020). *Cybersecurity in the AWS Cloud* (arXiv:2003.12905). arXiv. http://arxiv.org/abs/2003.12905

Souppaya, M., & Scarfone, K. (2012). Guidelines for Securing Wireless Local Area Networks (WLANs). *NIST Special Publication*, *800*, 153.

Steeneveld, W., & Hogeveen, H. (2014). *Characterization of Dutch dairy farms using sensor systems for cow management* (Vol. 98). https://doi.org/10.3168/jds.2014-8595

Steinert, M., & Leifer, L. (2010). *Scrutinizing Gartner's hype cycle approach*. 1–13.

Sussman, L. L. (2021). Exploring the Value of Non-Technical Knowledge, Skills, and Abilities (KSAs) to Cybersecurity Hiring Managers. Journal of Higher Education Theory and Practice, 21(6), 99-117. https://www.proquest.com/scholarly-journals/exploring-value-non-technical-knowledge-skills/docview/2563846494/se-2

Tarouco, L. M. R., Bertholdo, L. M., Granville, L. Z., Arbiza, L. M. R., Carbone, F., Marotta, M., & Santanna, J. J. C. de. (2012). *Internet of Things in healthcare: Interoperatibility and security issues*. 6121–6125. https://doi.org/10.1109/ICC.2012.6364830

Thakare, A., Lee, E., Kumar, A., Nikam, V. B., & Kim, Y.-G. (2020). PARBAC: Priority-Attribute-Based RBAC Model for Azure IoT Cloud. *IEEE Internet of Things Journal*, *7*(4), 2890–2900. https://doi.org/10.1109/JIOT.2019.2963794

The C2 Consensus on IoT Device Security Baseline Capabilities. (2019). Council to Secure the Digital Economy. https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf

The EU General Data Protection Regulation (GDPR). (2017). Springer Berlin Heidelberg.

The GSM Association. (2016). *GSMA: The Impact of the Internet of Things*.

The Modbus Organization. (2019). http://www.modbus.org/

There are officially more mobile devices than people in the world. (2014, October 7). The Independent. http://www.independent.co.uk/life-style/gadgets-and-tech/news/there-are-officially-more-mobile-devices-than-people-in-the-world-9780518.html

Thilmany, J. (2003). Alphabet Soup. *Mechanical Engineering Magazine Select Articles*, *125*(01), 44–46.

Thomas, G., & Myers, K. (2015). *The anatomy of the case study*. Sage.

Thubert, P., Bormann, C., Toutain, L., & Cragie, R. (2017). IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing Header (Request for Comments RFC 8138). Internet Engineering Task Force. https://doi.org/10.17487/RFC8138

Tschofenig, H., & Eronen, P. (2005). *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)* (Issue 4279). RFC Editor. https://www.rfc-editor.org/info/rfc4279

Tuttle, H. (2022). 2022 Cyber Landscape. *Risk Management*, *69*(1), 18–23.

Two Apple medical trials shed light on HealthKit. (2014, September 15). *Reuters*. https://www.reuters.com/article/us-apple-health-idUSKBN0HA0Y720140915

Uschold, M., & King, M. (1995). *Towards a methodology for building ontologies*. Artificial Intelligence Applications Institute, University of Edinburgh Edinburgh.

Van De Belt, T. H., Engelen, L. J., Berben, S. A., & Schoonhoven, L. (2010). Definition of Health 2.0 and Medicine 2.0: A Systematic Review. J Med Internet Res, 12(2), e18. https://doi.org/10.2196/jmir.1350

Vickery, C. (2017, June 21). *GOP Data Firm Accidentally Exposes Personal Details Of Nearly 200 Million Voters* [Interview]. http://www.npr.org/2017/06/21/533844095/gop-data-firm-accidentally-exposes-personal-details-of-nearly-200-million-voters

Vlamos, P. (Ed.). (2017). GeNeDis 2016: Geriatrics (Vol. 989). Springer International Publishing. https://doi.org/10.1007/978-3-319-57348-9

Wagstaff, K. (2014, December 5). *Sony Hack Exposed 47,000 Social Security Numbers, Security Firm Says*. https://www.nbcnews.com/storyline/sony-hack/sony-hack-exposed-47-000-social-security-numbers-security-firm-n262711

Wang, G., Atiquzzaman, M., Yan, Z., & Choo, K.-K. R. (Eds.). (2017). Security, Privacy, and Anonymity in Computation, Communication, and Storage (Vol. 10658). Springer International Publishing. https://doi.org/10.1007/978-3-319-72395-2

Wang, J., Pambudi, S., Wang, W., & Song, M. (2019). Resilience of IoT Systems Against Edge-Induced Cascade-of-Failures: A Networking Perspective. *IEEE Internet of Things Journal*, *6*(4), 6952–6963. https://doi.org/10.1109/JIOT.2019.2913140

Watts, S. (2017, September 22). *SaaS vs PaaS vs IaaS: What's The Difference and How To Choose*. BMC Blogs. https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/

Weiser, M. (1993). Hot topics-ubiquitous computing. *Computer*, *26*(10), 71–72. https://doi.org/10.1109/2.237456

Weiss, G., W. (2008, June 27). *The Farewell Dossier—Central Intelligence Agency*. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm

White, L. A. E., Krousel-Wood, M. A., & Mather, F. (2001). Technology Meets Healthcare: Distance Learning and Telehealth. *The Ochsner Journal*, *3*(1), 22–29.

Wieczner, J. (2017, July 18). *Hackers Just Stole $7 Million in a Brazen Ethereum Cryptocurrency Heist*. http://fortune.com/2017/07/18/ethereum-coindash-ico-hack/

Wilamowski, G., Dever, J., & Stuban, S. (2017). Using Analytical Hierarchy and Analytical Network Processes to Create Cyber Security Metrics. *Defense Acquisition Research Journal*, *24*(2), 86–221. https://doi.org/10.22594/dau.16-760.24.02

Williams, P. A. (2007). An investigation into information security in general medical practice [Doctor of Philosophy, Edith Cowan University]. https://ro.ecu.edu.au/theses/274

Williams, P. A. H., & McCauley, V. (2016). Always connected: The security challenges of the healthcare Internet of Things. *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, 30–35. https://doi.org/10.1109/WF-IoT.2016.7845455

Wong, J. C. (2017, November 22). *Uber concealed massive hack that exposed data of 57m users and drivers | Technology*. https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack

Wood, L. (2017, March 10). Global Sensors in Internet of Things (IoT) Devices Market 2016-2022: 100 billion IoT Connected Devices will be Installed by 2025 to Generate Revenue of Close to $10 Trillion. *NASDAQ OMX's News Release Distribution Channel*. https://www.proquest.com/docview/1875661837/abstract/ECA6E717076E4BB0PQ/1

World IPv6 Launch. (n.d.). Retrieved April 22, 2019, from https://www.worldipv6launch.org/

Yamin, M. M., & Katt, B. (2019). Mobile device management (MDM) technologies, issues and challenges. *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, 143–147. https://doi.org/10.1145/3309074.3309103

Yilin Mo, Kim, T. H.-J., Brancik, K., Dickinson, D., Heejo Lee, Perrig, A., & Sinopoli, B. (2012). Cyber–Physical Security of a Smart Grid Infrastructure. Proceedings of the IEEE, 100(1), 195–209. https://doi.org/10.1109/JPROC.2011.2161428

Yin, R. K. (Robert K.-Z. (1994). *Case study research: Design and methods* (2nd ed.). Thousand Oaks, Calif. : Sage.

Zhan, C., Hu, H., Liu, Z., Wang, Z., & Mao, S. (2021). Multi-UAV-Enabled Mobile-Edge Computing for Time-Constrained IoT Applications. *IEEE Internet of Things Journal*, *8*(20), 15553–15567. https://doi.org/10.1109/JIOT.2021.3073208

Zhu, B., Joseph, A., & Sastry, S. (2011). A Taxonomy of Cyber Attacks on SCADA Systems. *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, 380–388. https://doi.org/10.1109/iThings/CPSCom.2011.34

Zhu, Z., Lan, K., Rao, Z., & Zhang, Y. (2021). Risk assessment method for IoT software supply chain vulnerabilities. *Journal of Physics: Conference Series*, *1732*(1), 12051. https://doi.org/10.1088/1742-6596/1732/1/012051

10 APPENDIX A: IOTSOF

NIST Function	Unique ID	Additions / Alterations
Identify	ID.AM	• Expansion of inventory system for IoT Devices to have more than one identifier for asset management • When using software level identifiers, take advantage of hardware backed secure storage when possible • Ensure that module IoT devices can be grouped into a logical unit of parts for clarity of device make-up • When cataloguing devices, capture device firmware versions and manufacture revisions • Apply heightened vigilance to any cloud integrations directly with IoT devices • Capture any physical interactions an IoT device is responsible for • Include IoT training as a separate type of awareness training, similar to BYOD to ensure employees can identity IoT devices
	ID.BE	• Ensure that the physical actions of an IoT device form part of any analysis
	ID.GV	• Ensure IoT has its own distinct policies within an organisation
	ID.RA	• No Additional / Nothing to Add
	ID.RM	• No Additions / Nothing to Add

	ID.SC	• Be aware of and account for the potential difficult upgrade path of embedded IoT devices and systems
Protect	PR.AC	• If centrally managing credentials, ensure devices are integrated into existing access mechanisms o Utilise hardware backed secure storage for credentials whenever possible • If no hardware secure storage, ensure only administrators have access to credentials • Assume that any IoT device in isolated physical locations can be physically tampered with and compromised • Prefer device with either tamper-proof housings or tamper alerts • Wherever possible, ensure devices have uniquely bound identities for authentication and authorization
	PR.AT	• Deliver awareness training for IoT and its pitfalls, with identical principles as existing cybersecurity training
	PR.DS	• When present on an IoT device, utilise any TPM style verification of software • Strongly prefer hardware based cryptographic operations
	PR.IP	• Active simulation testing should include physical interactions of IoT devices when feasible • HR cybersecurity integration training for IoT should expand on general training to target organisation goals
	PR.MA	• No Specific Additions, Common Ecosystem Baselines
	PR.PT	• Restrict the ability to use removable media as boot location or as storage devices • Whenever possible, restrict all command-and-control traffic to an isolated network • Vet devices for their supported protocols, aggregation requirements and feature set

Detect	DE.AE	- Ensure that IoT devices have their own tailor alert thresholds when monitoring
	DE.CM	- Offload malware protections from IoT devices to more powerful devices where possible - Prevent unauthorised code execution - Implement cryptographic code verification for all update packages and services
	DE.DP	- No Additions / Nothing to Add
Respond	RS.RP	- Include IoT SME's in order of operations and personnel roles
	RS.CO	- Check regulatory requirements for any IoT specific reporting requirements
	RS.AN	- No Additions / Nothing to Add
	RS.MI	- No Additions / Nothing to Add
	RS.IM	- No Additions / Nothing to Add
Recover	RC.RP	- No Additions / Nothing to Add
	RC.IM	- No Additions / Nothing to Add
	RC.CO	- No Additions / Nothing to Add

11 APPENDIX B: IOTSOF-E

Ecosystem Characteristic	Considerations
Cyber-Physical Systems	Include all physical actions in any assessment of an IoT device
Organisational Maturity	Sophistication of deployments and resources will be bound by the organisation size and resources
Modern Cryptography	Use the most recent version of ciphers and protocols Use the largest possible amount entropy that is feasible when generating cryptographic keys Use secure and verified implementations of ciphers and protocols Follow a sliding scale of protections for both sensitive and regulated data
Secure Data Storage & Transmission	Store credentials and other sensitive information (e.g., personal/medical/financial) in hardware backed secure storage when possible Ensure that a device adheres to any regulations based on its function and the data it will be handling or storing
Endpoint Management	Ensure that all sensors are included in IoT device endpoints, as each sensor may be isolated from other sensors on the device
Device Reset & Refresh	Ensure that factory resets wipe all data from device and all associated support systems Ensure that a device refresh correct wipes system related data, leaving user data intact Ensure these operations can be performed remotely
Policies	Have dedicated IoT policies that cover the same areas as existing polices
Strong Defaults	What constitutes a strong default is sliding scale, based on secure protections required. Prefer manufacture set unique passwords on device delivery

	Change this manufacturer set password on initial device provisioning
Secure Provisioning & Updates	Ensure update packages are cryptographically verified, no matter the deployment type Deliver packages over a secure connection Ensure devices can recover remotely from a failed upgrade
No Deprecated Protocol	Use the latest version of a protocol possible and ensure that the version being used has no known public vulnerabilities
Hardware Secure Storage	If a device supports hardware backed secure storage, use it for any sensitive data
Authentication & Authorisation	Follow best practice, allowing for physical access and device communication windows