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.