2020

A Secure and Strategic Approach to Keep IoT Devices Safe from Malware Attack

Christopher Ray Murray
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Christopher Murray

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Jon McKeeby, Committee Chairperson, Information Technology Faculty
Dr. Cheryl Waters, Committee Member, Information Technology Faculty
Dr. Steven Case, University Reviewer, Information Technology Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2020

Abstract

A Secure and Strategic Approach to Keep IoT Devices Safe from Malware Attack

by

Christopher R. Murray

MS, Walden University, 2016

B.S., State University of New York at Canton, 2014

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December 2020

Abstract

Through the advances in technology, businesses can now utilize the Internet of Things (IoT) devices to improve workflow and provide better services to customers. However, without a strategy to secure these devices, Information Technology (IT) security professionals are left with vulnerable equipment. Grounded in routine activities theory, the purpose of this qualitative multiple case study was to determine strategies IT security professionals used to protect IoT devices in their environment. The participants were 6 IT professionals from 2 medium to large size healthcare facilities based in the Buffalo, New York, and the Washington D.C. area, who possessed strategies to protect IoT devices. The data collection included semi-structured interviews and analysis of 7 industry standardization documents and 12 business documents. Data were analyzed using cluster analysis; four themes that emerged included user education to promote security, protect the environment through security layers, a policy that supports security, and threats that the technical gaps present. A key recommendation is that IT security professionals develop a security strategy that uses multiple layers to protect IoT devices from malware attacks. The implications for positive social change include the potential for IT security professionals to implement multi-layered IoT security strategies, which can help decrease attacks on vulnerable IoT devices and assure citizens of protecting their data.

A Secure and Strategic Approach to Keep IoT Devices Safe from Malware Attack

by

Christopher R. Murray

MS, Walden University, 2016

B.S., State University of New York at Canton, 2014

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December 2020

Dedication

I dedicate this work to my best friend and husband Bruce A. Smith Sr., my mother Bonnie, my siblings Matt, Melissa, my support group Dr. Eliza Smith, Jake, Buddy, Jessica Andrianos, TreShawn, Nayia, Jasmine, Laura and family, LaVonne, Dick and Joanne, and my two cats Tommy and Lucy. You all have been my rock through the trials and tribulations of this degree. I remember telling everyone I wanted to get a terminal degree after getting my MSIT, and the amount of support was so overwhelming. You have always supported me in your ways- from your understanding for me sneak away and write while traveling to the Czech Republic, Las Vegas, and Thailand, to dealing with my mini meltdowns when I was overwhelmed. You have always been there for me. Words will never be enough to demonstrate my gratitude for you all. I truly thank you from the bottom of my heart. I would also like to dedicate this work to all of my Masonic Brethren.

Acknowledgments

I would like to say thank you to my committee, committee chair Dr. Jon McKeeby, my second committee chair Dr. Cheryl Waters, and my university research reviewer (URR), Dr. Steven Case. Your continued support and feedback will leave me forever grateful. Thank you.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

The ease of attacking connected devices are increasing more and more. It is necessary for security professionals to learn how attacks happen and prevent such attacks (Fu & Xu, 2018). It is critical to understand how to create and deploy policies and procedures that would best fit different environments.

Background of the Problem

Information Technology security professionals use policies and procedures to protect infrastructure and data (Aldosari, Snasel, & Abraham, 2016). These policies and procedures are based on the best practices or industry standards. In recent years, weaknesses in networks and devices were found to be a result of misconfigurations and lack of proper security controls (Majhi, Patra, & Dhal, 2016). IT professionals use best practices and industry-leading standards when looking to create standardization for processes or policies. The same consideration for networks and other devices should be used when Internet of Things devices are deployed.

Problem Statement

The increase in IoT devices being introduced into healthcare each year add more security vulnerabilities (Burns & Johnson, 2015). The 20 million projected IoT devices by 2020, in conjunction with the weak to no security controls in place, continue to increase the likelihood of a cyber-attack on IoT devices (Pishva, 2017). The general IT problem is a lack of strategies for how to protect the communication to and from IoT devices. The specific IT problem is that some IT security professionals lack strategies to prevent attacks on IoT medical devices from malware.

Purpose Statement

The purpose of this qualitative multiple case study was to explore strategies IT security professionals use to prevent attacks on IoT devices by way of malware. The specific population was IT security professionals with strategies to offset vulnerabilities in two medium-to-large-sized healthcare facilities in the Eastern region of the United States. The findings of this study may affect social change by emphasizing how users can use IoT devices to enhance their activities of daily living while remaining safe from hackers.

Nature of the Study

I selected the qualitative methodology as the research method for this study. Anderson, Leahy, DelValle, Sherman, and Tansey (2018) identified that in a qualitative study, the participants were part of the collection of the data, and questions were used to better understand the setting the participants work within. The ability to observe the participants in their work setting made the qualitative method the best choice for my study because the reaction to uncontrolled stimuli provides more raw data. With a quantitative method, the researcher looks for a setting that allows for phenomena and attempts to explains it with statistics or some other computational technique (Rutberg & Bouikidis, 2018). In this study, I used observations and interviews with the participants instead of numbers or computations to demonstrate the reaction to a response. Morse and Niehaus (2016) stated that the use of mixed-method looks to use the results of quantitative methods that also help support qualitative values with observation or vice versa. The mixed-method was not appropriate for my study because the statistical or hypothetical structure of a quantitative method was not applicable.

There are multiple qualitative designs, including: phenomenology, narrative, and case study. In case studies, a researcher investigates a specific environment that provides real-life scenarios (Cakmak & Akgün, 2017). In the study it was imperative that I could observe and understand the logic of the participant. Phenomenology is the study of how a participant experiences and understands phenomena (Kaivo-oja, 2017). There was not a need to address the perception of the participant about the phenomena to conduct the research. The narrative study, as discussed by Pauwels, Svensson, and Hirtenlehner (2018), examines historical and biographical information of the participant.

Research Question

The primary research question for this study was: What strategies do IT security professionals use to prevent malware attacks on IoT medical devices?

Interview/Survey Questions

1. How long have you been employed at your company?
2. How many years' experience do you have in cybersecurity?
3. What degree or certifications do you possess?
4. Is there a process for the policy to be created? If so, what is your role in the process approval?
5. Please describe the strategies you are utilizing to prevent attacks on IoT medical devices. What part did you play in the plan?

6. How are you preventing the things that motivate an offender to want to attack an IoT device?
7. What countermeasures do you have in place to prevent the user of the device from putting the environment at risk of an attack?
8. What is your current strategy for protecting data that may reside on an IoT device?
9. What is your process for responding to an attacked device? Has this process been tested? If, so how often and in what scenario?

Conceptual Framework

The conceptual framework that I used in this study was the routine activities theory (RAT), developed by Cohen and Felson (1979). RAT shows that the choice to commit a crime does not depend on how much money, the inequality of a situation, or if the person has a job or not. Instead, contemporary insights of society allow criminals the ease to act if the target was valuable and if there was a lack of protection. While the basic concept aligns and draws from the human ecology, the relationship between humans, and rational choice theory, which is the theory that states individuals make calculated decisions to make rational decision, it added value for the IT domain. The relationship between cybercrime and RAT is that the simple basis of not having protection in place and the reasoning for an attacker to conduct an attack.

To align the RAT theory with IoT security, the IT security professional should have proper security protocols to prevent the attack, which can prevent the attack from occurring. Using the concepts from RAT, the attacker looks at the lack of preventative measure(s) the IT security professional fails to put in place to prevent attacks (i.e., using Secure Shell (SSH) v1 instead of SSH v3) and builds an attack strategy. The attacker views the information they can obtain and determines if it is worth the attack (e.g., easy access to healthcare data). Lastly, the Routine Activity Theory is used to describe the motivation for the attack. For example, getting access to health records would provide the ability to gain other information like a DOB, illness, and other pieces to steal a patient identity.

Definition of Terms

I used the following terms throughout this study:

Big Data: The collection of large volumes of data to decide or to add value to other pieces of information (Grable & Lyons, 2018a).

Bring Your Own Device (BYOD): A device that is personally owned by an employee but is permitted to use for accessing company applications (Xuequn, Wang, & Heiko, 2017).

Honeypot: A decoy computer system used to proactively gather information from attempted attacks (Erdem, Pektaş, & Kara, 2018).

Internet of Things (IoT): Connections used to collect, compile, and transmit data for consumer use to help make decisions or stay informed (Hoffman & Novak, 2018). An object or “thing” is a device that is readable, recognizable, locatable, or addressable and would be connected to the internet (Gonzalez-Manzano, De Fuentes, & Ribagorda, 2019).

IT Security Professionals: For this study, this term included the chief information security officer (CISO), IT security manager, and IT security analyst, who were well-educated professionals and specialize in all the facets of information security (Whitman, & Mattord, 2018).

Malware: A collection of malicious code that is used to perform tasks that can be intended to cause harm to an infrastructure (Middaugh, 2016).

Assumptions, Limitations, and Delimitations

Assumptions

Lips-Wiersma and Mills (2014) identified that the concept of assumption uses information that does not need proof. My first assumption was that the participants would provide accurate answers. My second assumption was that the participants had the needed experience needed to answer the questions. My third assumption was that IT security professionals were motivated to implement a strategy that helped prevent attacks by using malware.

Limitations

A limitation is something that the researcher is not able to control and could negatively impact the research results (Busse, Kach, & Wagner, 2016). The main limitation was the intentional misrepresentation of the answer to prevent the possible work needed to implement a strategy. The other limitation could be the lack of experience to adequately explain the purpose or reasoning of how an IoT is or is not protected. Lastly, access to healthcare facilities were highly limited due to COVID-19.

The users that fit the criteria at additional sites were either laid off or were required to assume other responsibilities and were not able to participate in the study.

Delimitations

Thomas, Silverman, and Nelson (2015) explained that delimitations are used by the researcher to shape the scope of the study intentionally. In this study, my intention was to limit the scope of professionals to only IT security professionals in medium-to-large healthcare facilities in the Eastern region of the United States.

Significance of the Study

The usage of IoT is beginning to increase in sensitive areas of work that use valuable information, like healthcare (Wencheng et al., 2018). There have been studies and research conducted on IoT, but not enough in the healthcare sector. This study may be useful to IT security practitioners for the development of a strategy when implementing IoT or an improvement to their current strategies.

Contribution to Information Technology Practice

The purpose of this study was to explore the strategies being used by IT security professionals to protect IoT devices. The findings from the study may be used by the IT healthcare industry to avert potential hazards of having unsecured IoT devices. From a device manufacturer perspective, the increase use of IoT devices are great for the profit margins, but from a consumer and IT security professional's perspective, it was dangerous and costly.

Implications for Social Change

The contribution to positive social change comes from the need to protect the information that the users would access or provide in a healthcare setting when they are at doctor's appointment. The consumer base benefited from the safety and security of the data when they released the data to healthcare professionals. When people go to a healthcare facility, they share personal information and expect that the information will remain secure. The confidence from the consumer builds up when the data can remain protected. Users would be able to see the significance of protecting the information in other devices, like their own IoT (e.g., cell phone) to check lab results, which would also help to secure their data.

A Review of the Professional and Academic Literature

In the literature review, I focused on the research question: What strategies do IT security professionals use to prevent malware attacks on IoT medical devices? A literature review comprises critical thinking, evaluation of literary sources, and the process of synthesizing all the collected data (Badenhorst, 2018). In the literature review, I provided a breadth of knowledge on IoT devices and an in-depth review and synthesis of RAT. The focus of the literature review contains (a) Internet of Things and Security of IoT (57% of peer-reviewed citations), (b) RAT and rival theories – rational choice theory and lifestyle routine activity theory (22% of peer-reviewed citations). The complete references I used in the literature review are 80% of all references used in the entire paper.

Internet of Things

History of IoT

There are multiple ways to define IoT due to its ubiquitous usage. One definition of IoT is: connections used to collect, compile, and transmit data for consumer use to help make decisions or stay informed (Hoffman & Novak, 2018). An IoT system or device provides a mechanism for a series of devices or one device to connect in a networked environment. The concept of IoT is useful in many situations - for example, a smartwatch can be a convenient function to alert someone of a meeting. An IoT device can monitor heart rhythm for a heart irregularity while the patient is at home, possibly preventing a hospitalization (He, Cheng, Wang, Huang, & Chen, 2017). The use of IoT devices has a purpose in most daily activities, and when they couple with medical professionals, they are also now lifesaving tools.

At each turning point of technology, there has been a catalyst that has propelled technology to the next level. Throughout the centuries, there have been conceptual steps in the progression of technology. In the 19th century, the Industrial Revolution transitioned from making things individually to massive production called manufacturing (Jacobson, Spence, & Ng, 2017). The Internet Revolution, which brought about leaders such as Bill Gates and Steve Jobs, started the progression of technology. IoT is the next step of evolution for technology (Jacobson et al., 2017). Therefore, as technology advances, the expectation of the technology advancements provided forward progress and presented an opportunity for IoT to remain relevant.

Through the advancement of technology, and with more integrations into the user's work life and home life, the devices got smaller (Xu et al., 2018). IoT started with the use of systems reporting out to a device that could compile information and decide what information was needed and what to do with that information. IoT breaks down into four individual pieces that combine into one concept: obtaining the data, passing along the data, managing the data, and putting the data to work (Arshad, Azam, Rehmani, & Loo, 2019). Each of the components operates with a specific function the impacts the overall goal and carries out to the result. Once the IoT device get the data from the user or other source, it can evaluates how the data gets to and from the various devices (i.e., Bluetooth, near-field communication (NFC), or equivalent) (Arshad et al., 2019). It is the obtaining stage that has developed as the technology has improved (Arshad et al., 2019). The improvements in the obtaining step was developed as a newer technology was discovered and became available to users.

Next, the information must pass to a central repository. The passing can be a cellular signal from a phone, a wireless connection, or even a satellite signal. The information gets from an cellular tower or satellite to a server for the following steps to take place (Arshad et al., 2019).

The last two steps involve how the information is analyzed and delivered. Data management uses other technologies like Big Data or Cloud computing to provide an analysis of the information and begin to correlate information (Arshad et al., 2019). Lastly, the information is assembled into a user-friendly format to help the user of the device obtain or make decisions. The finalization part of the data looks at decisions made from other systems to present into an application or perform another action (i.e., another machine would begin a sequence of tasks; Arshad et al., 2019). The crucial steps in getting the information to a functional state for use in a decision system or for a user to perform and action.

While the use of IoT in different areas is becoming more prevalent, the ability to protect the devices and the information is also becoming a challenge. Due to the sensitive information that IoT devices can potentially use it, behooves an IT professional to apply layered security, like adding more than just a firewall or antivirus to protect a device (Moos, 2017). The underlying intention of IoT provides the interconnecting of devices to one another with little to no human interaction (Mendoza & Kleinschmidt, 2015). The concept of IoT and the layering of security are connected themes. The themes relate because of the close relationship of information passed to and from the user, plus the vulnerability of information's integrity, confidentiality, and availability.

A critical consideration of sending information across a network is to be sure the information is secure. The protection of the information as it sends from a central location to an IoT device has an impact on how the device is secured, especially in vital usage, for example, implanted devices in humans or external devices that control medication (Arias, Wurm, Hoang, & Jin, 2015). An attack on a device can be critical, but the inability to remove the threat and have a later attack occur is even more dangerous (Arias et al., 2015). The security of the information at the device level adds an extra layer of concern for security professionals (Rghioui & Oumnad, 2017). The devices bring information to the user's fingertips and provide a more seamless and less cumbersome experience. Therefore, the securing of IoT or any other mobile device improves the awareness of unexpected, unpatched, or malicious devices that may exist, and in return, protects the infrastructure and data on the network.

As IoT devices become more involved in daily business and personal routines, the attack surface for the data on those devices becomes larger (Khan & Salah, 2018). The devices used to make up the IoT environment places the best of smart connectivity and computational power of context-aware technology through networked resources (Nayyar & Puri, 2016). As information moves from one location to another, the chances of interception and manipulation of the data increase, and the integrity of the data could potentially decrease (Dysart, 2018). Therefore, securing the devices did not need users and corporations; it was a must to ensure that data remains secure.

Bring Your Own Device

Bring your own device (BYOD) is the process of bringing your personal device to perform specific business tasks (Cho & Ip, 2018). The use of BYOD has improved the adoption of various technologies that businesses have sought to use (Cho & Ip, 2018). The adoption of technology can assist with the productivity of the business and security constraints found in users using unfamiliar technology to perform a business task. The use of BYOD has increased in the last 2 years. The increase can be closely related to the IoT devices that help users maintain schedules, add to improving processes, or improve familiarity with equipment (Magruder, Lewis, Burks, & Smolinski, 2015).

The use of a BYOD allowance introduces an increase in potential problems (e.g., patch management) and places an even higher need to identify critical assets (Aminzade, 2018). Aminzade (2018) found that critical assets have detrimental effects on the business if compromised. A variety of newer products have improved the adoption of BYOD. These devices include laptops, cellphones, or smartwatches. The BYOD introduction has also enhanced the use of programs that could otherwise be annoying from the user's perspective (Magruder et al., 2015). The use of personal devices can be a helpful resource for employees and cost-effective for businesses.

Bringing your computer, smartphone, or tablet to work for business is becoming a common trend in various industries (Xuequn et al., 2017). In most industries, a policy needs to be developed and applied to personal devices for business transactions (Krombholz, Hobel, Huber, & Weippl, 2015). The intent is to ensure that the information accessed from the employee’s personal device can be secured (Chalee, Soontorn, Ekkachan, & Visut, 2017). The combination of BYOD and instilling a reliable method of obtaining the data creates a holistic approach to advancing technology and ease of user experience.

To address the vulnerabilities and protect a company’s environment, IT professionals need to have control over what users may download to their BYOD devices (Dang-Pham & Pittayachawan, 2015). One viable option to BYOD is using a corporate-owned and personally enabled (COPE). COPE, as determined by Feigelson, Jim, Serrato, and Jonathan (2016), is when the organization provides a cell phone or tablet to an employee, who can tweak it and utilize it for both business and individual purposes. Therefore, the use of devices is meant to be helpful, but can also pose a risk to the security of business infrastructure, so the IT security professional should weigh the risk factors should decide if BYOD is best for the current environment.

The ability of the users to make changes on the device poses a security risk. As cell phones continue to store sensitive information and represent a greater danger of theft or burglary, required controls must be organized to avert or relieve potential data theft (Leclercq – Vandelannoitte, 2015). The need for companies to secure how their data is transmitted, stored, and destroyed on BYOD is not only a standard, but a requirement (Baillette, Barlette, & Leclercq-Vandelannoitte, 2018). The struggle for IT professionals to secure the data on devices is increased when users can bring in their own devices (Baillette et al., 2018). If a company wants to entertain the BYOD experience it is important for the IT security professional to solidify policy or procedure to protect any data on a BYOD or COPE. The use or improvement of the policies by the IT security professional can decrease the risk of data theft or malware infection.

Because a user could bring in a device, good policies around BYOD would help support any change needed for the user's device and provide scalability of advancing technology within the company, while keeping the data secure. However, Chatfield and Reddick, (2018) stated policies that are too cumbersome or create frustration for the user began to find ways around the policies or restriction. A struggle with personal devices can be the lack of applications and expertise within the company that could help defend the BYOD devices as laptops or computers have (Belanger & Crossler, 2018). Regardless of the environment, the data must be a priority, and the building of policy and procedure that users would be able easily circumvent is equally inefficient as not having policy and procedures. Furthermore, while this concern or struggle applies to most environments, it holds a significant interest in fields that house vital data (e.g., healthcare).

Healthcare IoT

Healthcare is becoming one of the biggest adopters of technology in order to improve the outcome of patient's conditions. The use of IoT or mIoT (Medical Internet of Things) has doubled since the introduction of the pacemaker in the early 1990s (Yi & Cai, 2019). The driving factor in the integration of IoT into healthcare has been the freedom it has provided patients. Previously, a patient would need to come in for monitoring and would sometimes stay overnight stay or longer. Now, the patient can set up a remote monitoring tool (e.g., mobile electrocardiogram), and the information would transmit back to the doctor's office or have it record on the device and be retrieved later (Lakhoua, 2019). These advancements in technology have improved the patient experience and provided a sense of empowerment to the patient.

The integration of IoT into service-oriented industries has increased the innovation of different services. IoT started to change how the healthcare industry uses technology and change how clinical decisions are made (Hoyme, 2017). The concern for IT security professionals is the security of information and what protections exist for its transmission (Owens, 2016). The security controls for the information as it is added to the world-wide web are essential but should couple with proper product mapping and patch management; to ensure that the devices have the newest software and is compatible with appropriate security protocols (Anderson et al., 2018). The use of IoT in service-oriented areas is becoming more accepted. Still, the need to secure or develop policies that ensure the data is always secure is a must and, in most cases, regulated.

Because the exposure to electronic personal health information (ePHI) exists with the use of IoT and medical information, the need for proper securing of data is imperative. Hospitals need to know when a threat to their data exists and how to handle the threat (Owens, 2016). The ability to see how devices rate from a security perspective is essential and would prove helpful when there are questions related to the hardening of the device (Hossain, Islam, Ali, Kwak, & Hasan, 2018). The hardening of the device and software provides another layer of security (Hossain et al., 2018). The hardening of the device removed or makes it more challenging to gain access to information transmitted to or from the device and any data that currently reside on the device (Anderson et al., 2018). The presence of only having the policy on the protection is essential but does not prevent the data loss, so the need to have software and hardware hardening is crucial to the protection of the data and, therefore, should align with policy.

The use of IoT medical devices is beginning to help patients live more fulfilling lives (Ellouze, Rekhis, Boudriga, & Allouche, 2018). The ability to restart someone's heart with an implanted defibrillator has made IoT medical devices a must-have in the medical field (Ellouze et al., 2018). Medical devices have unique features that have functions for the patients, and a medical device typically needs to be programmed before it can be used on the patient (Ellouze et al., 2018). Furthermore, IoT medical devices improved patient's daily activities when discharged from a hospital, and in some cases, did not require a night stay at the hospital for observation.

The lifesaving capabilities plus the vulnerabilities have placed medical devices on the radar of IT security professionals, and these devices have much information that can fatally wound someone. Ellouze et al. (2018) stated that having four areas to break down and look at the techniques used to protect the device: the first one served as a link or gateway between the device and the patient using the device. The second is based on the credentials that the programmer would use to access the device (Ellouze et al., 2018). The third is a lightweight approach that helps to omit let energy-aware security techniques that would reduce the cost. Lastly, the fourth used the physical proximity to the device before it can be programmed. With all these techniques combined, the use of healthcare IoT can deploy in such a way that users and the data remain protected and provide the best clinical information possible.

Embedded systems and security

An embedded system serves as a programmed device and has a function to a more extensive process (Ebert & Dubey, 2019). The purpose of an embedded system is to perform a private function (e.g., a network switch) that would take a significant amount of general-purpose processing power (Shukla, 2019). Embedded systems are available in a variety of industries, but the ubiquity of embedded systems have not caused a need for a security measure to improve (Elmiligi, Gebali, & El-Kharashi, 2016). The consumer-level use is no different from enterprise-level use, and at each of these levels, the user, whether it be in a BYOD environment or in an enterprise area when the company provides a mobile device, the security concerns still exist (Elmiligi et al., 2016). An embedded system attack happens in a variety of methods: reverse engineering, cloning, spoofing, and other methods (Elmiligi et al., 2016). Elmiligi et al. (2016) describe that understanding how to classify an attack could help with preventing attacks.

Figure 1, as described by Elmiligi et al. (2016) there is a representation of a model that would help place a possible identifier on the attacks and areas that would need to consider during the integration of an embedded system.

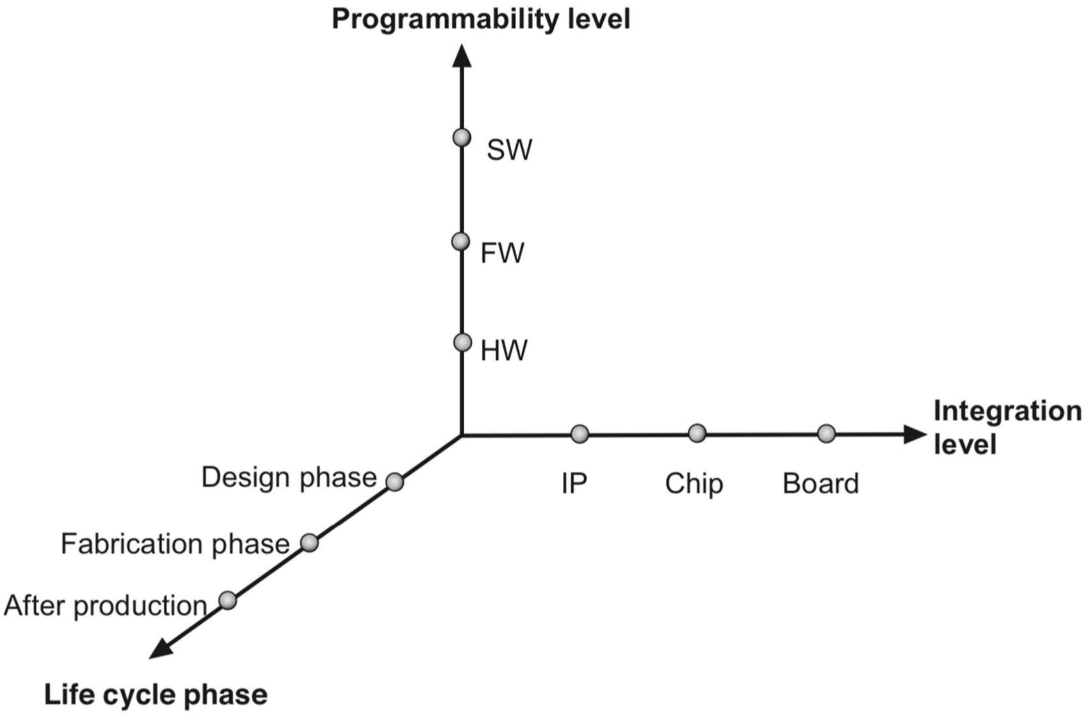


Figure 1. The evaluation of embedded systems based on each of the parts that could have a vulnerability. Copyright permission in Appendix A. Retrieved from Elmiligi, H., et al., (2016). Multi-dimensional analysis of embedded systems security. Microprocessors and Microsystems, 41, 29–36. https://doi org.ezp.waldenulibrary.org/10.1016/j.micpro.2015.12.005

The IT security professional would need to consider each stage in the area and would need to be remedied before moving to the next part (Elmiligi et al., 2016). For example, threats on the firmware (F.W.) part, it would need to fix that vulnerability before moving to the software (S.W.) phase. The help of a framework provides a structured evaluation to establish a policy or procedure. Likewise, the use of Figure 1 helps describes how an embedded system is evaluated based on individual parts that could be vulnerable. However, the usage of the security framework like the CIA could help other instances that did not meet the multi-dimensional representation.

Personal Identifiable Information (PII) / Protected Health Information (PHI)

Protecting information about customers, patients, and employees is a vital aspect of information security. PII is the link or linkable piece of information to a natural person (Ducich & Fischer, 2018). PII is protected by laws such as the Healthcare Insurance Portability and Accountability Act of 1996 (HIPPA) and the 'Children's Online Privacy Protection Act of 1998 so that it does not provide access to unauthorized users. Likewise, PHI is evermore protected and equally sought out for by a hacker for malicious intent. One reason for the highly sought information is the value it holds. The value of a medical record or information about a patient from a medical record is worth substantially more than a Social Security Number (Soma, Courson, & Cadkin, 2009). One cause of the difference is the ability of multiple use cases from the criminal. For example, if a hacker were to access information about a patient that contained medical information along with the date of birth, Medicare ID, and address, the hacker could falsely file healthcare claims faster and with more accuracy than with just a Social Security Number and get more financial gain (Cohen & Mello, 2018). The prevention of access to information is not as simple as just encrypting records. Good IT hygiene involves technical but also behavior improvements (Jang, Jung, & Park, 2016a). The data can have the best technical security, but if it is handed out by an ill-informed employee, the technical changes would not matter. The combination of technical and behavioral or cultural changes helped in the effort to secure patient data.

Security of IoT devices

As the technology advances, the user's demand for more devices that are connected to more sensors increased and therefore increased the attack surface along the way (Guerar, Merlo, Migliardi, & Palmieri, 2018). As IoT devices become more immersed in various industries, there more vulnerabilities discovered for IoT devices (Sha, Wei, Yang, Wang, & Shi, 2018). Likewise, the increase of the IoT use changed the behavior pattern of the users of the device, and the way information gets collected and stored by the user required a change in how data needs to be secured (Weber, 2015). Beresford, Mascolo, and Gruteser (2018) stated that the landscape changed and what begins to get attacked changed as well. From the attack on a vending machine, like the one in 2017 where a universities vending machine was used to conduct a denial-of-service attack, to an attack on Minecraft servers, a popular online game where players build their own environment and invite others to join their "world" to help build. At times these attacks are based on the popularity, and other times it is based on primary oversight of the security of the device. The data that sends or transmitted must remain safe, regardless of the device, and this becomes a more significant challenge when using BYOD or devices that cannot be controlled by a security professional.

Confidentiality, Integrity, Availability (CIA)

The CIA (confidentiality, integrity, and availability) triad applies when evaluating the IT risk of a device, framework, or policy (Aminzade, 2018). The implementation and balance of the CIA are one of the most challenging tasks in an IT risk assessment (Aminzade, 2018). The information provided for implementing the CIA has not controlled information and is known by cyber-criminals, who can use this information to gain access to vital infrastructure approaches and other methods of preventing a breach (Aminzade, 2018; Dorogovs, 2016). The use of the CIA in the grand scheme of security and the development of policies provides a standard for IT Professionals to use. One of the most common forms to disrupt the confidentiality of the data is the misuse of passwords (Gřivna, & Drápal, 2018). Hackers look for an easily guessed password (e.g., Password1) to attempt in a typical attack called Brute Force, where the attacker is just guessing, or have a program guess, a variety of different passwords until it is correct (Gřivna, & Drápal, 2018). Another part of the triad of CIA is integrity, and it, too, has a pivotal meaning when being used to evaluate a streamlined process or a new policy. When implementing a policy that pertains to confidentiality, integrity, or availability, it is essential to understand the application and the guidelines. To understand how to apply or what guidelines to use, and IT security professionals should understand the application of the three parts of the triad and what role each play in the securing of information. The first in the triad is confidentiality. Confidentiality is the preservation of access to information and the disclosure of the information (Dempsey et al., 2011). The application of confidentiality is essential when determining who has access to data and at what level of security needs to be applied to protect the data (McCallister, Grance, & Scarfone, 2010a). The application of confidentiality may provide a better foundation for a policy, as the support and assistance in its use are standardized amongst multiple sectors. The second part of the triad is integrity. Integrity is the reference to how the data remains in the purest form and is not manipulated or altered by an improper or unauthorized actor (Dempsey, Witte, & Rike, 2014). Integrity also means the data is always proven to be the same data that the original creator provided, and if changed, the person that changed it can be identified (Dempsey, Witte, & Rike, 2014). The last part of the triad is the application of availability. Availability describes how often the application or system is available. There are a variety of methods to use to ensure the system is available (i.e., redundancy, shadowing, or a RAID configuration) (Nieles, Dempsey, & Pillitteri, 2017). Availability provides assurance or reassurance that the systems were available when they are needed or required. The overreaching goal of CIA is to make sure that allowed user accesses the information or system, accurate information can be obtained and trusted from the system, and that the system is always available – or at least not taken down by malicious events.

The integrity of the data or systems where the data resides altered by manipulating the outcome of the data or how the system works in such a way that it "cheats' the integrity of its intended use (Gřivna, & Drápal, 2018). For example, the manipulation of gambling games or machines can be made so that the user(s) benefit by changing the mechanism of the algorithm in the machine (Gřivna, & Drápal, 2018). Lastly, availability is the ability to get the data or system when the user needs the information and is the last balance of the triad to make all three work together in harmony (Sosin, 2018). The use of the CIA is shown to have assisted in the creation of policies that have best practices and industry standards to support the logic.

The purpose and development of the confidentiality, integrity, and availability triad for a company builds around the understanding of how removing one or two of the components caused the triad to fail and therefore place the company at risk. The cybersecurity sector has a lot of different interests, and understanding how one attack crippled a business can help another from becoming a victim as well (Sosin, 2018). When the CIA is implemented, there needs to be a defined method of understanding the risk that is involved, if any, of the three components that are not met and what that meant for the overall protection of the data or device (Sosin, 2018). The method of creating a policy that only addresses some, but not all components, is just as problematic as not having one at all.

Malware

Malware is software that is built by a hacker or entity that is made to break a system by destroying the files or spying on a user or group (Iannarelli, & 'O'Shaughnessy, 2015). The intent of sending implementing a malware attack is to either disrupt service or business (Keese & Motzo, 2005). The attack can be sent via an unsuspecting email, removable media insertion into a machine, or by getting access to a user account. The use of malware is also used to bring a business to a stop because of perceived or actual bad business practices. This kind of use is when companies that do testing on animals or other controversial topics gain the attention of "hacktivist" (He et al., 2017). At any rate, the protection of the data and prevention of malware to get in is critical in providing confidential data, a business that has data integrity, and available business.

Signes-Pont, Cortés-Castillo, Mora-Mora, and Szymanski (2018) agreed that the problem with identifying malware is its ability to hide in any source (i.e., attached to an email, within a document, links associated to messages). The amount of damage malware can also because depended on the target (Signes-Pont et al., 2018). If the target(s) have a weak detection protocol for malware and no or poorly delivered awareness training for end-users, the likelihood of the malware payload will succeed (Signes-Pont et al., 2018). Furthermore, the awareness of vulnerabilities in the infrastructure impacts what security policies and procedures need to be enacted to protect the environment from malware.

The concerns of malware in the healthcare arena should move IT Professionals to adopt better policies and processes. Various issues plague the healthcare field when it comes to a medical device, the internet, and protected health information (Middaugh, 2016). When a health record is stolen and then used for another person's identity, the integrity and confidentiality of the medical records are violated (Middaugh, 2016). The instance of losing a medical record or having a breach of multiple records puts in question the appropriateness of the current process and policies that should have prevented the loss or breach to happen (Middaugh, 2016). The education of the healthcare industry with best practices and lessons learned from other incidents provided a clearer understanding of how policy and process could prevent loss of data or breach of the data. It assumes that just removing all access to the system is better, but removing a segment of the network, or all the network, from the visibility from the outside is not a fix to prevent attacks. The attack or breach of a network is the first of many steps to add malware or to cause harm to the infrastructure (Guri & Elovici, 2018). Throughout the events from well-known attacks like Stuxnet, where a malware payload is delivered by a USB inserted by an insider, the ability for the attacker to gain access to the environment has been proven easier than expected (Guri & Elovici, 2018). The encouragement for physical security and the prevention of hardware to circumvent policies and procedures is becoming a necessity.

The spread of malware can have an impact on the response time and, in return, determined how fast and what resources are needed to stop the attack. To define how to react to an attack, the IT security professionals must know the scope of the attack and what is in the environment (Nikolopoulos & Polenakis, 2017). A measurement criterion needs establishing (e.g., epidemic model). Models, such as an epidemic model, are used to describe the state of the machine and helps with understanding the (a) status of the machine, (b) status of the malware, and (c) ability and the likelihood of resolution of the attack (Nikolopoulos & Polenakis, 2017). Because the scope and the status of impacted devices surface and organized, the IT security professionals can make a better decision on how to prevent, isolate, and stop an attack.

The propagation of malware depends on the expertise used to create it and how good or bad the attack surface is patched or protected (Nikolopoulos & Polenakis, 2017). The securing of devices in these situations is even more critical as the attacker has the advantage due to uncontrollable environment variables (Nikolopoulos & Polenakis, 2017). To that point, controlling how the users connect and what connections are allowed on the chosen device provides more control to the IT Professional. For example, if the user is attempting to connect to an open-unsecured wireless connection and checking work documents or applications, the users would not be permitted and would have to connect to a virtual private network first.

IoT Malware

With the introduction of IoT devices, various industries have been a victim to attacks from relaxed or nonexistent security protocols. WannaCry and Petya are the two latest malware infections that have influenced clinicians and healthcare establishments all over the world (Jarrett, 2017). The devices used in a healthcare setting are generally for transmitting data or serving as a sensor (Anggorojati & Prasad, 2018). The increase of the IoT devices requests in the healthcare industry and the lack of protection to the devices made for a dangerous combination.

Therefore, aligning a strategy that would work for all, including, IoT would be an ideal situation for IT security professionals (Erdem, Pektaş, & Kara, 2018). While an antivirus or firewall is not possible to install on an IoT device, the use of other strategies like a Honeypot, which is a decoy computer system that is used to proactively gather information from attempted attacks (Erdem, Pektaş, & Kara, 2018), would help identify potential attack patterns or types of devices targeted (Erdem et al., 2018). The Honeypot would take an IoT device and insert it in what seems like a legitimate environment but would instead be a non-critical location that cannot see other critical systems, and then monitor the traffic to capture any wrongdoing. In return, the traffic provided data to the IT security professionals to help protect how the devices are getting attacked (Erdem et al., 2018). The combination of traditional network security (e.g., firewalls, intrusion detection systems, etc.) in addition to Honeypots, the IT security professionals would be able to secure the devices and prevent malware from accessing the sensitive data.

Security Best Practices

Encryption. Understanding what endpoints are in the environment helped with understanding the level of threat or risk in the event a breach occurred. The awareness of the endpoints helped established the potential content on the devices, which, in return, determined the level of risk if compromised. The basic principle of securing hardware from being compromised is to provide a level of isolation that prevents the attacker from accessing information across the applications and the hardware of the device (Schaumont & Montuschi, 2018). Keeping up with the everchanging threats from hackers can be a daunting task. However, having a reliable security standard established needs to be broad enough to cover the applications, hardware, and other connected devices. A standard method of ensuring the isolation of information is encryption.

The premise of encryption is to keep the content secure from people not intended to see the message is referred to as encryption in transit. The process of protecting the message can vary from case to case. One method of protecting the message is to use asymmetric encryption method with a public key. Using this type of method would begin with creating a symmetric key that was used to encrypt and decrypt the information (Khan, & Salah, 2018). The essential factor is that one person, the sender, only know the decryption key. Another method of encryption is after the message has arrived and additionally encrypting the message on the received device, referred to as encryption at rest. Muslukhov, Sun, Wijesekera, Boshmaf, and Beznosov (2016) stated that using a four-digit code or a password is not enough to secure data that is at rest, and encryption is critical. When accessing data that is encrypted, the IoT device and the storage device need to authenticate. Muslukhov et al. suggest a process known as a Sidekick System. In this system, there would be a library that would keep the ‘keys’ for the IoT device to unlock the data from the storage devices. The storage device and the IoT would sync to this library and could understand what the keys are being used. Figure 2 outlines a basic workflow of how the Sidekick Library process would work. The importance of the Sidekick Library is that it compartmentalizes the authentication to a central location and helps protect the confidentiality, integrity, and availability of the data.

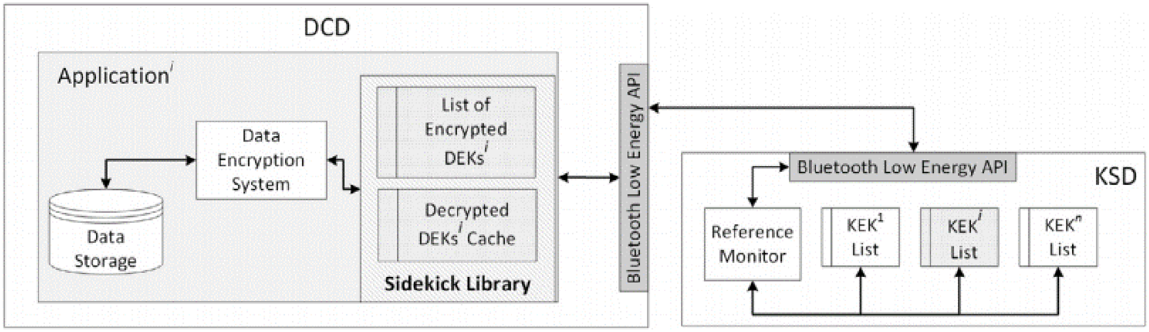


Figure 2. Muslukhov, I., Sun, S.-T., Wijesekera, P., Boshmaf, Y., & Beznosov, K.(2016). Decoupling data-at-rest encryption and smartphone locking with wearable devices. Pervasive and Mobile Computing, 32, 26–34. https://doi-org.ezp.waldenulibrary.org/10.1016/j.pmcj.2016.06.016

The encryption process can occur in a hardware or software environment (Stapleton, 2019). In either hardware or software, a positive and a negative is presented in using one versus the other. In a hardware environment, the decisive point is that the key that controls the encryption and decryption of the data is better protected because of the hardware's physical and logical controls (Stapleton, 2019). Likewise, if the hardware encryption was networked or connected to other devices, the concern of latency or delays become a problem when encrypting and decrypting the content (Stapleton, 2019). The use of hardware encryption modules has better-controlled protection to the content that is stored on the machine locally on the hard drive of the device.

In contrast, if the encryption process utilizes a software encryption approach, the hardware being used is assumed not to have any hardware encryption. When using software encryption, as compared to the hardware encryption, the key that controls the encryption and decryption process is stored outside the hardware being used (Elnaggar & Chakrabarty, 2018). An immediate concern with using software encryption is the integrity of the key used to encrypt and decrypt the data. The risk is much higher for the key to becoming compromised, and the detection of a compromised key is difficult, and the inability to determine the integrability of the key possesses significant risks (Elnaggar & Chakrabarty, 2018). The use of encryption has its pros and cons, and the IT security professional should be able to base the decision on what worked best in the current environment. As with most technology, it is not always a one-size-fits-all approach, and adjustments from the IT professional and the users were needed.

Patch Management. Like encryption, the use of patch management to mitigate vulnerabilities is a necessity in an IT security professional's arsenal. Patch management is the ability to ensure that the hardware and software are at its best for the user's experience, security, and interoperability with new installs of code, scripting changes for application performance, or increases in security to ensure the user and data remain safe from attackers (Dennis, 2018). When hardware and software get designed, the developers have the best intentions to release the best version of hardware and software.

However, to remain at the top of the interoperability scale and ensure that it continues to work with other applications and hardware, updates are needed (Anderson, 2018). Updates also provide required changes to the hardware and software to address any security and interface improvements from known bugs. The process of managing the patches varies from one company to another company.

The best example of how patch management can prevent damage to vulnerable systems is WannaCry. In early 2017, the exploit called WannaCry left thousands of systems vulnerable. The feat took advantage of a protocol called Server Message Block (SMB) (Anderson, 2018). The SMB protocol was used to help spread the malware across file shares on the target network. The connective nature of file shares reached multiple devices and files shares that relied on SMB to carry out information. Approximately one month before WannaCry was discovered, Microsoft had a patch out called MS17-010 that fixed this vulnerability (Dennis, 2018). If companies maintained a tight schedule for patch management, machines would not be likely to be vulnerable to the WannaCry exploit (Dennis, 2018). Most environments have a process for patch management, and most have methods of adjusting to critical patches that come out.

Nevertheless, most also do not have a method of patching their IoT devices (Bertino et al., 2016). The problem that is faced in Healthcare is that some of the IoT devices are implanted in a human, and taking it out is not safe nor secure. The volume that healthcare facilities are using IoT devices are climbing and will outnumber the total number of P.C., laptops, and people combined (Ka Man, Mei Na, & Chun Kit, 2015). The IoT devices are being used to also track the other software in a facility (Minoli, Sohraby & Occhiogrosso, 2017). However, the management of the IoT device alone has no practical method of getting patched with updates and security vulnerabilities and is a manual process.

IT security professionals should have a policy in place that defines what is allowed on a network and what is not allowed (Cox, 2019). Also, Cox (2019) found that the facilities that had a policy in place about what devices could be connected to the network were not enforcing it, or the users had no idea it even existed. The underlining concern appears to be the inability to (a) see the IoT devices that are on the network and (b) how those IoT devices are managed for security vulnerabilities and patches. The need to manage IoT devices is more than an asset management purpose. The need also comes from the threat assessment perspective. Multiple demonstrations provided on how criminals could take over a thermostat and hold it hostage until a ransom is paid (Cox, 2019). In a hospital setting, this is critical and bring an entire hospital operation to a halt. It is not possible to see into the future to address the feat, but a proactive and consistent approach to patch management would have certainly assured better adherence to the security update Microsoft pushed out.

Asset Management. According to the NIST cybersecurity framework (Calder, 2018), asset management is the first step in understanding what needs to protect in an environment. The management is not only associated with the device, but also the applications, people, and role that someone would play in the cybersecurity arena (Al-Moshaigeh, Dickins, & Higgs, 2019). If the device can link a user, and the user can link to workflow, then the type of data and the value associated with that data can be assessed. The benefit of assigning a value to the device, and the user provides a standard of how that device would need to be protected (Al-Moshaigeh et al., 2019). If the user was a lower-level employee that had low-level access, then the security need could be a standard GPO structure, password expiration, asset tagging, and proper Active Directory security groups. While on the other side of the spectrum, if there were a Chief Financial Officer that had a device, it would be given a higher level of protection: applications that have two-factor authentication, encrypted hard drive/removable drive, data loss prevention policies audited, and RAID drives, etc.

According to Boeckl, Fagan, Lefkovitz, Megas, Nadeau, O'Rourke, Piccarreta, and Scarefone (2019), IoT devices are "black boxes" that cannot manage like a traditional machine (e.g., computers, server or switches). The is difficult to track the IoT devices that reside on a network and even more challenging to patch those devices (Boeckl et al., 2019). All of the precautions used and security standards can provide a safer environment for laptops, P.C., servers, and other commonly used hardware. The difference is the use of the same methods to protect IoT devices that are used to protect other hardware (Díaz López et al., 2018). One of the most significant gaps is the ability to find applications and hardware that can protect IoT devices with the same protections as a laptop, P.C., or server (Díaz López et al., 2018). Nine attack surfaces are considered relevant for IoT device that the Open Web Application Security Project (OWASP) has identified as the most the concerning, and that should be addressed about the management of the devices once they are in the intended environment:

- Administrative interface – does the device have one, and is it protected outside of the typical default username and password
- Device web interface – this is what houses all the configuration and is accessible via web access
- Mobile application – this can be any application that the IoT device may interact with or provide data to and from
- Device network services – these are the networks that the IoT device will work on
- Update ability – this looks at the ability for the devices to receive updates (i.e., firmware, security, virus)
- Devices physical interface – this references the embedded chipset that the IoT device uses to communicate
- Devices firmware – this references the application or logical statements that exist to allow the device to function

- Locally stored data – any information that the devices store on locally

All the topics mentioned above provide a way for the attacker to access the device. These are also vulnerabilities that cannot solve with a piece of software or hardware. A layered approach should exist to ensure that all aspects of security (Díaz López et al., 2018). The lack of management for IoT devices places an administrator in an awkward position. An environment variable can render the device inaccessible and, therefore, impossible to manage. One method can be used to help control what devices are allowed, and that is called whitelisting. Whitelisting allows the administrator to allow or prevent a device from connecting to the network or a computer. Mendez and Yang (2018) stated that whitelisting devices allows the administrator to control what information can pass through the IoT to the computer. The use of whitelisting adds another level of management for the devices.

Furthermore, an IT security professional should use a variety of methods to detect vulnerabilities within the infrastructure. A key point to ensure that systems remain updated and free from known vulnerabilities is to understand how encryption works, maintain a schedule for patch management, and asset management (Kohout, Komárek, Čech, Bodnár, & Lokoč, 2018; Dennis, 2018; Anderson et al., 2018). The use of preventative security measures helps an environment remain secure, but the same processes and protocols are not always possible on IoT devices, and therefore, a layered approach should be used (Erdem et al., 2018). IoT devices do not share the same CPU and memory capabilities that a traditional computer or laptop would have, and proper asset control and policies need to fill the gap where the technology may not.

Routine Activity Theory. RAT was developed by Lawrence Cohen and Marcus Felson in 1979. Cohen and Felson (1979) theorized that trends in crime were indicative of patterns in conduct called routine activities. The activities defined by the reoccurrence of the events and could apply to a variety of instances (e.g., social interactions, leisure, shelter) if they were part of an everyday routine (Cohen & Felson, 1979). Also, Cohen and Felson (1979) described that routine activities could happen at home and work. Like this, the victim and offender had to be connected, such that their space and time had to meet to create an event that a likely offender, suitable target, and the absence of a capable guardian existed (Cohen & Felson, 1979). Furthermore, the connection of all three components made the crime possible and can be a basis on how to prevent such crimes.

The development of RAT was intended to look past another theory of human ecology that Hawley developed in 1950 (Cohen & Felson, 1979). Cohen and Felson took Hawley's approach and had a similar thought process but differed in the scalability. Hawley believed that crimes were on three pillars: rhythm, tempo, and timing (Cohen & Felson, 1979). The understanding and application of RAT assisted in the shaping of how strategies can be developed to prevent malware attacks on medical devices.

The definition of routine activity is the ordinary activity of someone that does provides a service to a population or individual need (i.e., making food, providing shelter, social interaction, learning) (Cohen & Felson, 1979). The service helped provide a criminal a purpose for committing a crime to that service or that person providing the service. For example, if the district manager of a financial firm were known to carry large amounts of money on them, a criminal would find that person a definite target to rob. Alternatively, if a CEO had a laptop for work and he left the laptop in his unlocked car, that too would be a good target.

However, for any of the mentioned events to be worth the criminal's time and effort, the need for an offender to meet in time and space to a victim would be required according to RAT (Choi, Earl, Lee, & Cho, 2018a). A single event or series can help increase or decrease the likelihood of the victim meeting the offender, and therefore the crime being committed. The act of a crime cannot remove because the victim is on the Internet or using other forms of technology. The initial approach of RAT was that the victim and the offender had to meet in a place through a time and space combination (Cohen & Felson, 1979). With the advances in technology, the meeting of the victim and offender online is made possible. The advances in technology have also made it possible for the victim to visit a manipulated site, where an offender would be hiding to perform some malicious acts, like stealing a credit card or other information (Reyns, Henson, & Fisher, 2018). Overall, the RAT intends to evaluate what attracts the offender to the victim and how those attractions can be prevented or offset with policy or procedure.

Also, a variation of RAT has been theorized by a more recent researcher that encompasses Cohen and Felson's (1979) RAT framework and helps align modern technology with RAT. Such a theory was hypothesized by Choi (2008) and referred to as Cyber-RAT. Similar to the traditional RAT framework, Cyber-RAT also identifies that there are additional components that direct the genesis of online crime: (a) the concept of a digital guardian, such as security programs, measures, or policies; (b) the online vocational or leisure activity such as a social network or messaging services that bring two or more people together (Choi et al., 2018a). The creation of Cyber RAT stemmed from the combination of lifetime exposure theory and routine activity theory, respectively. The combination of the two theories states that the lifestyle online and the capable guardianship may increase or decrease someone's chances of getting victimized (Choi, 2008). The routine uses of online messaging service, group forums, or other patterns in conjunction with the lack of some computer security introduce risk. That same user may also be more likely to click on links or download attachments from offenders from those chat rooms or forums that they visit (Choi, 2008). The combination of the research of Choi (2008) with Cohen and Felson (1979) provides a framework that has been used to shape crime prevention policies in the traditional community to those crimes that occur in the virtual community.

The premise of RAT works around three components that are paramount to the definition: a motivated offender, a suitable target, and a lack of guardianship. The terms are flexible in that other literature with different verbiage (e.g., suitable targets may be an opportunity), but the concepts are the same. Using RAT, by definition, if one of these components is missing, a crime is imminent (Hawdon, Costello, Ratliff, Hall, & Middleton, 2017). According to RAT, the crime cannot exist if the target has a way to prevent an attack (i.e., using a virtual private network when connecting from the outside of the company, ensuring IT is updating the virus database on the user's machine, or not leaving a laptop in plain sight in a car). The breakdown of RAT and each of the elements is helpful to understand the overall approach of this study and how the application of RAT is applied.

Motivated Offender. The motivated offender was the ‘criminal' in most cases that committed the crime(s) and caused harm to another person or situation (Schnell, Grossman, & Braga, 2018). The motivated offender looked at a person or situation to find how he or she best gained from their actions. If the offender can conclude that the victim(s) are weak and vulnerable, it may appear easier for the offender to strike at one, as opposed to another (Schnell et al., 2018). Therefore, understanding the motivation of a person looking to cause harm or the potential to cause helped align any policies to prevent the situation from the beginning proactively.

The purpose of the motivation can be described in a multitude of ways: from a societal to a rational manner, but at any rate, the purpose is to visualize how a situation can remove the motivation for the offender. From an individual perspective, the motivator can look for gender-based or educational-based motivations (Bergmann, Dreißigacker, von Skarczinski, & Wollinger, 2018). The gender assumes that males visited websites that are riskier than women (e.g., pornographic), and educational motivation is used when looking at those that are less informed about proper identification in various types of fraud (Bergmann et al., 2018). Whatever the motivation may be, understanding how that impacts (e.g., gender or educational) most of the user group helped a better policy creation and, in return, assist in protecting the data's infrastructure and company.

Suitable Target. Without someone to commit the crime against, the criminal does not have much to loathe for when looking to make a profit or gain other desires if there is not a suitable target. In the findings from Cohen and Felson (1979), a suitable target was one that provided the object that the criminal desired. The ‘value' of the object that the criminal is looking for correlates to the concept presented by Felson and Clarke (1998), which outlined the acronym VIVA (value, inertia, visibility, and access). The acronym helped describe why one target would or would not be more likely sought out than another. The value of the target is viewed as a financial value or the worth of having the information that places others at a disadvantage. In either situation, the target has access to the information or money that encouraged the illegal move forward and commit the crime, regardless of the consequences (Felson & Clarke, 1998). If the target has a routine that does not deviate and the criminal knows the route and routine, it is possible for the criminal to create a situation that would trap the target and not provide a way to escape.

If the victim can escape easily, then the offender would have to put in more effort to prevent that from happening, and knowing the routine and route would improve the offender's chances of not losing the victim (Felson & Clarke, 1998). In comparison to inertia, visibility provides the offender with the ability to watch or see how the victim behaves or reacts to specific events (Felson & Clarke, 1998). However, the contrast is that visibility also pertains to gathering information about the victim from a variety of outlets (e.g., social media and networking with others that know the victim). The term access is literal in its definition. It defines how easy it is for the offender to get access to the victim, in both the physical and virtual sense. Felson and Clarke (1998) define the term access as the ability to carry out the illegal act. All these definitions combine to provide the ability to outline how and what determines a suitable target for the offender. VIVA also provides a way for the policy and process creators to prevent a suitable target from becoming 'interesting' to an offender. All of which can be helpful when developing a plan for a policy or how to harden a system.

Lack of Guardianship. Guardians are those that look to protect a person or a group from becoming a victim. Hollis, Felson, and Welsh (2013) changed how the term guardianship was thought of and placed a term of ‘handler' to the guardian. The handler would be someone like a teacher, parent, security officer, or in a corporate environment, an IT security professional. Guardianship expresses that by ensuring that would-be offenders do not get access to the potential target (Hollis-Peel & Welsh, 2014). If the guardianship is not present, the likelihood for the offender to commit the crime is higher. Creating such an environment that a criminal would not want to attack removes the urge for criminals to act. In the design of such an environment, the ecological thought process would help take the focus off the group that is looking for protection (Nikitkov, Stone, & Miller, 2014). The creation of a policy that increases the hardening of a target and one that prevents the offender from viewing the target as something to pursue helped remove the initial interest and therefore lessen the chances of victimization.

Rival Theory – Lifestyle Routine Activity Theory. The Lifestyle Routine Activity Theory (LRAT) stated that the use of probability would determine if a target engages in specific behavior, then the chances of them becoming a victim increase (Pratt &

Turanovic, 2016). With the use of RAT, if any of the three elements (likely offender, a suitable target, and lack of capable guardian) are missing, then victimization would not occur (Cohen & Felson, 1979). On the contrary, LRAT outlines that if any of the three are present, then the crime would happen (Pratt & Turanovic, 2016). The chances, or probability, of a crime happening versus removing a key that would cause crime is not the focus of the study. The focus of the study is to look at how establishing a policy around protecting IoT devices from malware improves or does not improve the security of the data and the device (Sung, 2019). The importance of understanding the decisions a victim would make does have an impact on lessening the crime occurring or not. However, LRAT highlights the probability of risky behavior taking place as the primary factor of the criminogenic (Van Ouytsel, Ponnet, & Walrave, 2016). The use of LRAT dictates that certain behaviors, in general, can result in crime happening but does not provide a framework that would clearly outline how an approach of protecting IoT would prevent the crime.

The importance of why someone would plan would be based on how victimization could occur (Reyns, Henson, Fisher, Fox, & Nobles, 2015). For example, if a college student decided to go out and drink without telling someone where he was going, and went to a location he was not familiar with, LRAT would say that victimization probability would be higher. Also, the use of the connection between social inequality and victimization is answered with LRAT (Choi et al., 2018a). Therefore, the outlook with LRAT looks at how the summation of socio-economic and routine activities could increase the victimization.

The use of LRAT would not provide a framework strong enough to shape around its use around the creation of a policy for IT security professionals. The expansion of RAT added another part called proximity to crime (Engeström, 2018; Cohen & Felson, 1979). The addition looks at how crime is increased because someone lives in a crime-ridden neighborhood. Cohen and Felson (1979) focused on how and why the crime occurred in certain areas. A postulation made by Cohen and Felson (1979) highlighted that crimes that occur do not happen at random. The structure of RAT and LRAT are similar, and both serve a purpose. However, it would be best suited for the IT security professionals to conceptualize the policy around better-aligned points like what entices the criminal, what makes the victim appear vulnerable, and how the data can stay protected. All of which is captured best with RAT.

Rival Theory – Rational Choice Theory. Rational choice theory (RCT) is the concept of self-directed methods of performing an act to obtain something that is desired. The theory was developed by Derrick Cornish and Ronald Clarke (Cornish & Clarke, 1986). The initial purpose of the theory was to apply it to the development of crime control policies (Cornish & Clarke, 1986). The theory focused on how and why a criminal would decide to commit a crime. Bransen (2001) posited that choice of the act is not based on events, but is a deliberate decision made by a capable who thought of all the possible outcomes. Furthermore, the use of the RCT has its place in the prevention of crime holistically but does not provide the details needed to support a policy creation.

The use of RCT evaluates the benefit and the punishment or the risk and reward balance. If the offender feels that the risk outweighed the benefit, then the crime is not performed (Özdemir, Tanhan, & Özdemir, 2018). In the application of RCT with a sex offender, Gönültas, Oral, and Beyaztas (2015) found that those that committed sexual abuse crimes made a point to think about how their decisions would impact their life, and found that the criminals believed that the benefit was higher than the risk. As described, the use of RCT provides an outline of criminal and the choice to commit the crime, but it does not describe the framework to prevent such decisions.

Overall, the use of RCT is helpful and adds value to the prevention of crime, but itself cannot provide enough information and foundation to develop processes and policies. However, the use of RAT assists with the development and understanding of how the process and policy can prevent crime from happening (Schnell et al., 2018). RAT does so by understanding why the criminal is interested in the target (i.e., how much information does the target provide to the public, or is there too much information about projects available), and places precautions around the vulnerabilities (i.e., does the communication to and from the medical devices encrypted and on a segmented network).

RAT Theory/CYBER RAT in Use. The holistic insight of RAT evaluates how a criminal may choose to commit a crime. While in no way is it possible to stop all crime, using RAT helped identify what policies and procedures can be used or changed. The use or change of a policy or procedure merely establishes a baseline for a company to protect an asset. RAT can be viewed as an opportunity-based theory, and therefore one that helps establish why a specific action should or should be taken (Schaefer & Mazerolle, 2017). The application of RAT also identifies the crime or event that can happen and how it can be avoided to protect an asset (Schaefer & Mazerolle, 2017).

Specifically, RAT looks at the actions that increase the effort, lower what a criminal would get from the crime, reduce the motivation to commit the crime, and lastly, the excuse of evening committing the crime (Schaefer & Mazerolle, 2017). Schaefer and Mazerolle (2017) evaluated the RAT in what was termed 'waves. In each wave, there was an indication that placed meaning on RAT. In the first wave, the need for time-space was paramount for a crime to happen. In the second wave, Schaefer and Mazerolle (2017) discussed how the merging of the three pillars (offender, place, and victim) could be avoided by placing a controller at each point. The last wave looked at the use of guardianship as a whole and indicated that if it did not exist, then crime would happen, and if it did, then crime did not happen (Schaefer & Mazerolle, 2017). All of the waves were used to help understand how Schaefer and Mazerolle (2017) developed the 3R's that were also placed in a triangle like the second wave but was done in a combined approach of all three of the waves and places a level of variability to how certain crimes may happen and others may be stopped. In the end, the result of preventing the crime was the expected outcome, and understanding where that prevention would be placed resulted in the creation of the hypothesized fourth wave.

Likewise, Hawdon et al. (2017) indicated that not only did the use of RAT maintained relevance with the three pillars of a motivated offender, suitable target, and lack of guardianship; there were also conflict management, target suitability, and victimization. The extension of RAT, according to Hawdon et al. (2017), illustrated that the use of additional behaviors not only helped prevent the occurrence of offenses but was also able to help remove the crime from that location. Using the logic from Hawdon et al. (2017), the use of conflict management in a cybervictimization case would be to ignore or delete the text or email simply. In a non-cyber event, the suitability of a target can be based on how easy the offender may think it would be to take physical control of a person would increase or decrease the likelihood of a crime (Hawdon et al., 2017). Victimization is increased or decreased by implementing a way to remove the offender and the asset the offender is after. While there are various methods of removing the offender and changing the want of the asset, the underlying issue is how can this be performed without the potential victim has to live in a bubble.

Victimization contains a large group of purpose and reasoning of who, why, and how people are victims of crime. As outlined in a study conducted by Wick et al. (2017), gender is not a primary factor any longer when looking at cyber-victimization. The focus of the cyber-crimes are around the value of the target and the adjustment that needs to be made on the criminal based on the accessibility of the target, attractiveness (if they are worth the attack), and if they are the right person that had the needed target (Wick et al., 2017). The use of RAT in this study evaluates how cyber-harassment can be avoided by using preventative measures and stopping the risky behaviors that entice criminals. This same concept can be used to develop policies and procedures to protect the data and those that are custodians of the data.

Unlike the victimization that is traditional in a physical sense, the application of RAT can be applied to the cyber environment just the same. The attacker is not one that always someone that fits a stereotypical outline. In reference to an attacker, Bock, Shannon, Movahedi, and Cukier (2017) see this shaping into an IP address or the last location of the computer used to prepare for an attack (i.e., a distributed denial-of-service attack). In a study conducted by Bock et al. (2017), there is a close connection with the time that the attack happens and the weaken in which is being exploited. The weakness is a delay in patching, lack of resource, or some other information that the attacker may aware of from either social engineering or another mean of gathering data. In the study, attackers would pick a time of the day that would allow their traffic to 'blend' in with other high traffic on the network and make it harder to identify. The use of RAT was used to understand the timing of the attack.

In another study that was conducted by Ming-Li and Shun-Yung, (2018), the use of RAT was used to highlight how cybercriminals used the online suitability and attractiveness of ATMs in Taiwan because of the lack of guardianship. The criminals were able to steal over $2.6 million from banks by only using malicious code or malware to force the ATMs to 'spit out' money. The study found that, like most criminals, financial gain was the goal of their actions. The issue that is discovered with this study is that the capture of these crimes has the Internet to hide who they are and add another issue for authorities (Ming-Li & Shun-Yung, 2018). The need for technology is an understatement and is needed for the financial sectors to remain secure from attacks such as these. In all, the application of RAT can help identify for the companies where weakness exists in their current infrastructure and open the discussion on how to fix the weakness.

Transition and Summary

In section 1, there was a detailed exploration of IoT devices and how those devices work in a variety of environments. Also, there was an outline for the lens that the study is going to use. The use of the RAT was used to align the application of the study to a framework. The use of RAT describes how the three factors - motivated offender, a suitable target, and lack of guardianship - can collectively help prevent a crime from happening by placing policies and procedures to reduce the risk.

The literature review focused on IoT, how IoT has impacted Healthcare, what malware is, and how malware has changed the use of IoT in Healthcare. Lastly, the literature review focused on the use of routine activities theory in comparison to other theories and why it was better suited for use in this study. By using the routine activities theory, it was possible to understand how IoT devices are vulnerable and how they can be protected. The next section provided a detailed landscape of the study, such as research design, methodology, population, and sampling.

Section 2: The Project

In Section 2, I explain in detail the research method, design, and processes. I define the role of the researcher, the participant selection process, population and sampling, and ethical research. Lastly, in this section, I cover the data collection, organization, the process for analyzing the data, and the reliability and validity of the study and collection of the data.

Purpose Statement

The purpose of this qualitative multiple case study was to explore strategies IT security professionals used to prevent malware attacks on IoT devices. I focused on leaders in the IT security field that resided in Washington D.C., and Buffalo, NYof the United States and implemented a strategy to address the prevention of malware on IoT devices. The positive impact for society was implementing a strategy to prevent malware on IoT devices and enable freedom from unauthorized access of IoT devices.

Role of the Researcher

In this qualitative study, my role was to collect and analyze data and present the results in an unbiased and impartial manner. Ensuring the participants that the information would be safe and confidential data and handled appropriately was critical to provide the safest environment to divulge such information (Morris, Armstrong, & Balmer, 2009). I structured the interviews to provide an opportunity for the participants to express their expertise on the topic of creating a strategy around securing IoT devices in a healthcare setting (Jacobson, Brackbill, Frazier, & Gargano, 2019). I selected the participants based on their use of a strategy, regardless of its level of success.

Furthermore, the use of IT security professionals in the healthcare industry, whom implemented a strategy, dealt with security breaches, and had insight on why such a strategy can be valuable.

I have worked in healthcare for 6 years. Most of my experience has been in IT security and operations, protecting data. One year was spent on the clinical side, helping patients. The amount of data that transversed through the hospital was unsurmountable in size, and the protection of that data was paramount for the patient and the hospital. There are structures and standards to protect data in medical record systems (i.e., encryption, network segmentation, etc.). The significant gap was recognized when the protected data went on an IoT device (i.e., insulin pump, infusion pump, ventilator, etc.). The problem was that information would be encrypted from the computer would not be encrypted from the IoT device due to the hardware (Yang, Zheng, & Tang, 2017). Lastly, the use of a strategic approach to secure IoT devices protected the data, provided continued confidence to the patient that their data was safe, and instilled reassurance that the information the clinical staff receives was accurate.

While conducting this study, I followed the guidance of the Belmont Report. I used the Belmont Report to ensure that the three core principles of beneficence, respect for persons, and justice were met while the study was being conducted (United States Department of Health and Human Services, 1979). United States Department of Health and Human Services (1979) stated that the three principals of benefice, respect for person, and justice remained a priority during the study. Therefore, I explained the potential risk to participants that was associated with the study.

I used a recording device and a transcription service to ensure that I did not inject bias into the participant's responses. Greenwood, Kendrick, Davies, & Gill (2017) stated that the use of the audio and creation of the transcription was a helpful aid in ensuring that information was accurate and was not changed to prove a point in one way or another. To help remove bias, I conducted an in-person interview or through video chat. The medical facility had no affiliation with my current employer. The researcher needs to ensure that their views on topics can be removed (Fusch & Ness, 2015). No other researcher conducted research in this study, and I remained open-minded to any ideas brought forth. In addition, Castillo-Montoya (2016) indicated that by using the interview protocol a researcher would control the precision of the data saturation and give an organization to the researchers questioning. I interviewed three participants at each facility in the Washington D.C. and Buffalo, NY region of the United States until I achieved data saturation.

Participants

In this study, participants were in Washington D.C. and Buffalo, NY of the United States and were employed at a medium to large (2,300–10,000 employees) sized healthcare facility. The participants were an IT security professionals who had a minimum of 2 years in IT security experience. The participants created or helped create strategic policies surrounding the technical landscape and the IoT devices therein (i.e., IT Security Manager, CISO, CTO, CIO, ISSO, or equivalent). Lastly, the facility employed the participants at least 2 years in their current role. The role and experience of the participants are significant to the study, so both criteria were used when providing feedback. Preston, Leone-Sheehan, and Keys (2019) explained that the participants are used to help drive the understanding of the topic and add clarity to already supporting information from the study.

At the start of the interview, I used opening questions to help establish a level of comfort for the participant (i.e., how long they have worked at the facility, their education, and experience, or equivalent). Franks (2017) explained that helping the communication remains comfortable for the participant would improve the value that was provided. If the participant made jokes to help relax the situation or complains about a specific issue, the acknowledgment or demonstration of acceptance helped get better quality information. These cues may be minor but can help build the rapport between the researcher and the participant. The communication between myself and the participants was professional, and the participant always had the option to stop the interview at any point during the interview.

The gatekeeper provided me access to the participants throughout the interview process. As I work through the process, the gatekeeper assisted me with access to documents, processes, or policies, if permitted. Due to the access, the gatekeeper has access to critical information, and I leveraged that relationship to build participation from other participants; therefore, providing an overall positive experience for myself and the participants. Each participant had an opportunity to ask any question RD before the interview by email or phone. As Newton (2017) outlined, when dealing with information about the participant, the trust relationship needed to be clearly defined to help retrieve needed information. I began the interview with demographic questions. The questions were followed by open-ended questions about the topic of strategy around protecting IoT devices in the healthcare arena. O'Cathain and Thomas (2004) stated that the point of using open-ended questions was to give the participant a chance to add information that may not have been asked in a closed-ended question. The point that I drew from a question later helped me in building the structure of the study.

I conducted interviews via Zoom due to the large distance between the sites and me. The gatekeeper provided me with a list of email addresses. I sent each participant an email that outlined the premise of the study. Attached to the email was a letter of consent that provided details of the study. After the participant agreed with the study, a reply email was sent with data and time that worked. I created a Zoom link that matched the date and time and sent it to the participant. At the designated date and time, I had my webcam on and microphone enabled. I introduced myself and thanked the participant. I informed the participant that the interview would be recorded and that they could stop the interview by letting me know.

After the interview, I explained the recording would be kept confidential, and no identifying information about the person or the company would be provided to the public also, that the recording would be kept on an encrypted device. I also said that I would be transcribing the interview and conducting a follow-up meeting to ensure accuracy in my transcription. After each of the interviews, I sent each participant a letter thanking them and a copy of the transcripts. I set up a second interview, via Zoom, and reviewed the transcripts with the participants. Lastly, I used the information obtained during the conversation, business documents, and industry-standard information to compile my findings.

Research Method and Design

A qualitative multiple case study was best suited for strategizing to prevent malware on healthcare IoT devices. Boddy (2016) explained that when a qualitative method was used, the researcher needs to have a clear understanding of the subject matter to ensure that a high degree of the body of knowledge exists. It was for that reason that I was able to organize the information obtained through interviews, research, and other forms to develop a study that outlines the preventative methods of malware on IoT devices.

Research Method

For my study, I relied on the participant's professional feedback and experience and capturing the information in a qualitative multiple case study, which I conducted by interviews. It was common for researchers to use qualitative interviews to obtain data from the participant's interview (Vasileiou, Barnett, Thorpe, & Young, 2018). The data was directly from a source that would meet the eligibility requirements of the study. I used a qualitative interview method to help convey information in a more mature manner (Vasileiou et al., 2018). Therefore, the method of qualitative research worked best for this study. Another benefit of the qualitative method was evident in the need to ask for additional information or clarifying information from that participant. I used probing questions that helped clarify information from the participant.

Likewise, inductive reasoning provided background, analysis, and context behind the participant's feedback (Vasileiou et al., 2018). In this study, I used inductive reasoning to outline the participant's usage, implementation, and other reliable strategies surrounding securing IoT devices from malware. The use of the qualitative method provided an opportunity for me to hear what the participant(s) must share their experience and its value to the study. The ability to evaluate the feedback from the participant were critical when using the qualitative method, as it helped delineate any exiting assumption from the participant (Peterson, 2019). Understanding why a participant who creates or implements a strategy, views the topic in a certain fashion, was imperative to the overall focus of the study.

I considered the use of a quantitative method. The premise of a quantitative method looked to quantify data and place a generalization on those results, which was used to measure the incidents in which the study occurs. Park and Park stated the statistical information was used to form conclusions and are typically descriptive. The use of a semi-structured technique to collect (i.e., like an interview) helps align the information from the participants with the goal of the study (Park & Park, 2016). While the use of statistics and quantifiable data were important, it does not provide an insight into how implementing or not implementing a strategic plan to protect IoT devices from malware attacks happens.

I also considered the mixed-method approach, as it includes both qualitative and quantitative methods. Schoonenboom (2018) explains that a method of research was selected based on the overall-reaching purpose of the study and what was expected from the answers that are provided by the participants. In this study, both factors were relevant to answer the study question. Unlike quantitative methods, my study consisted of open-ended questions, and I did not use a survey of the participants to collect data. While using a mixed-method could be helpful in cases where a complex and a higher level of data was needed, it would not serve helpful in my study and did not use mixed-method. As noted by Meister (2018), the use of mixed-method demands more time to address both aspects of quantitative and qualitative methods, and this study does require that level of attention, which explains more why the mixed method was not considered for my study.

Research Design

Due to the exploratory nature of this study, using a case study was better than an ethnographical or phenomenological approach. I used a case study approach which helped in getting more than one instance and a variety of evidence and provides a use-case design to explain and describe a phenomenon in more detail (Sampson, Goodarce, & O'Cathain, 2019). As such, a case study was going to help outline the multitude of events and answer the overall research question, all of which could be achieved easier with a case study than with the other design structures.

Ethnographic and the phenomenological design was considered but I found them to not best suit the study. The use of an ethnographic design indicates that the researcher would be looking for information relevant to the participant's heritage or cultural behavior (Tierney, 1985).

Furthermore, it demonstrated how a case study would best fit this research. The use of an individual occurrence was not needed for this study. It was more important to look at the corporate level and how the strategy was or was not being used to secure IoT devices from malware.

Population and Sampling

The population for this study was IT security professionals ranging from IT security manager, CISO, CTO, CIO, ISSO, or equivalent depending on the structure of the strategic process within the two healthcare facilities that were selected in the North Eastern region of the United States. A gatekeeper, as described above, was used to help coordinate the participants. Malterud, Siersma, and Guassora (2016) described that the selection process of a population was to have the most relevant information possible without needing to go beyond the defined population. Therefore, selecting the correct participants was vital to the success of gathering information from the participants. The selection of the participants was dependent on the best participants that fall into these roles at the respective location - IT Security Manager, Director of IT Security, Chief Information Security Officer, Chief Technology Officer, Chief Information Officer, or Chief Compliance Officer, have two or more years in IT security have been employed at the facility for two years. The facilities were selected on the size of the facility and the location. A conference room was virtual in a Zoom environment. I told the participant that the meeting would be held in Zoom, and no one else was partaking in the interview. The facility was not within a 100-mile radius of the selections to ensure that no conflict of interest. Lastly, each of the participants had experience and knowledge of implementing a strategy to minimize the attacks on IoT devices with malware.

Sampling

Determining to sample was important. There are a variety of methods to use to determine the sampling. A researcher can use simple random sampling, where the researcher gives each person in a population a number. Cho, Jang, & LoCascio (2016) indicated that a selection process would be that each of the numbers given was placed on a table (i.e., 200 people in the population, so numbers 0-199 are placed on a table) the table was turned on the wheel. The number that was stopped on was the selection, or something was thrown at the table (i.e., a dart) to select the number. This method would not help because I have defined group, and using this method would not be needed. Another method of sampling was systematic sampling. Ashwood, Vanguelova, Benham, & Butt (2019) indicated that systematic sampling would ensure that a specific number of participants are selected from the given population. For example, if there are a total of 1,000 people in the population, and the researcher needed 100, the researcher would use the following mathematical formula 1000/100 = 10th. So, this would indicate that every 10th participant would be used in the research. Using this method would be helpful if my population size was larger than 100, but it was not and, therefore, would not add value or purpose to the selection process. The participants in this study are identified by title and experience.

Another method that was considered was called stratified sampling. Stratified sampling was used to select the appropriate amount of data points for the population to maximize important information (Tong, 2006). Uribeetxebarria, Martínez-Casasnovas, Escolà, Rosell-Polo, and Arnó (2019) indicated that using stratified sampling would help decrease the cost and time by using an optimized sampling size as opposed to larger and more irregular sizes as well as provide more proportionate sizes respective to the population examined. For example, with random selection sampling, there would be a population size of 100 from Company A, 400 from Company B, and 800 from Company C. If random sampling was used, the number of participants would be lower compared to each Company A size and the selection process would skew. If using stratified sampling, then a selected subset of each Company was taken. For example, 10 participants taken from Company A, 20 taken from Company B, and 40 taken from Company C. Using the stratified method would help ensure a more proportionate number of participants. In this study, the IT professionals may be lower in smaller company size than a larger and, therefore, would negatively impact the sampling. While stratified sampling was beneficial, it would not help in this study, as the group was narrowed enough by the experience requirements and the title of the position. Lavrakas (2008) indicated that a census was the total count of all people in a population. The use of census sampling collects data from everyone in the population of choice. Because the population selection process was to experience and title, the collection of data was specific enough to collect data from all participants and not be too cumbersome for the collection process.

Therefore, the sampling of the population was census sampling. Census sampling was the sampling of all populations that meet the eligibility requirement (Tobin, Nugroho, and Lietz, 2016; Hosseinabadi, Karampourian, Beiranvand, & Pournia, 2013). One of the benefits of using census sampling was using more than one establishment (i.e., four different healthcare facilities) (Charman, Petersen, Piper, Liedeman, & Legg, 2016).

Arias-Gómez, Villasís-Keever, and Miranda-Novales (2016) included that the inclusion process of the participants based on their eligibility in the study. Therefore, the participants needed to have two years' experience in the IT security field, implemented or prepared a policy focusing on the prevention of attacks on IoT devices, and be willing to participate in the study to be eligible. In addition, the exclusion of participants focused on those that are not willing to participate in the study and withdraw. The eligible participants were interviewed by phone or in person. In either scenario, I allotted 45 minutes for questions and follow up discussion. Ensuring the process adheres to all official guidelines, an interview protocol was used (see Appendix B). The outlined interview protocol followed, and I used the same questions and process for all participants. The participants signed the consent forms, which outlines what the study consisted of and that all their personally identifiable information was not disclosed at any time during or after the study.

The ability to confirm the message and information the participant provides during an interview was critical to the validation of the study. Caretta and Pérez (2019) indicated that to attain validity, the process of repetitive conversation confirming the information improved the validation of the content. In addition, while the process of doing validation can be time-consuming and financially draining, it was important to a study (Caretta & Pérez, 2019). The process I followed was similar; I collected the information from the participants and conducted a follow-up interview reviewing the conversation.

Ethical Research

The use of ethics in research was important. To ensure that this study complied with ethical standards, I ensured that the privacy of the participant was always forefront. McGlothen, Cleveland, and Pados (2019) stated that there are four parts of ethical principles (a) nonmaleficence, (b) beneficence, (3) justice, and (4) autonomy. Owonikoko (2013) defines the four ethical principles as such: the use of nonmaleficence, which was a twined process of benevolence, was the understanding the no one in the process of the study was hurt; the other was benevolence, which was the outstanding moral perspective that others are kind; justice was treating participants fairly; and autonomy, or respect for people, indicates the ability of competent subjects be able to make their own decisions, along with being recognized and respected. These practices in the study use clear communication on the next steps, consent forms, and the ability to withdrawal from the study at any time. To protect all participants involved in research, Walden uses an Institute Review Board, IRB, to provide oversight to the research process. Biros (2018) indicated that providing the participant with a method to give consent ensures they have ethical rights.

The consent forms were signed, and a copy was provided to the participant for their records. A five-year holding period will be kept, along with the other documentation for this study. Information that identifies a person or a company was confidential and must remain (Lippe, Johnson, & Carter, 2019). Ensuring that participants have the confidentiality needed, each participant was provided a masked titled (i.e., Participant 1). Also, the company's name was masked with a similar naming convention (i.e., Company

1). Lastly, I obtained Walden's IRB approval before I collect any data from the participants; to this point, I took the guidance of Walden's IRB to ensure that I meet and maintain the highest level of ethical research. All the participants in my research were able to withdrawal from the process at any time, and the participants acknowledged the withdrawal and other processes by reading and signing a consent form before the research was conducted. However, the participant would be able to withdrawal from the study after they signed the consent form. I did not provide any incentive for the participant to proceed or continue with the interview. The use of money to get someone to participate would result in the negative result of information and negatively impact the results. (Ripley, 2010). There was no use of money for participation in this study.

For the protection of the company and participant, the names of each were disguised with a pseudo-name—the names aligned with the order they are interviewed (e.g., Participant A and Company A). The use of masking the data helps with the protection of the participant and the company (Surmiak, 2019). The information that was collected was stored on an encrypted drive that was password protected that only I had access to and was kept in a locked cabinet. The information was stored for five years after I get the CAO approval to ensure the highest level of confidentiality was met. As I am collecting the information, the names, phone numbers, email addresses, names, and addresses of all the parties were not shared with anyone. Before I started collecting the information, I sent an invitation to the participant along with a consent form. The invitation, found in Appendix C, asked the participant for their cooperation and had the consent letter attached. Both documents were signed and returned to me before the interview began.

Data Collection

Instruments

The use of data in a case study can vary. Yin (2014) stated that the focus of data should derive from around the four principles of conducting a case study: the use of multiple sources, creating a database, making a connection between the data points, and the careful approach of using electronic sources for data. In my study, I was the primary source for collecting data. My questions were asked in an open-ended manner, to help elicit more information and prevent short one-worded answer. The use of open-ended questions was framed to gather short or long answers to identify a correlation within the observed environment (Weller, Vickers, Bernard, Blackburn, Borgatti, Gravlee, & Johnson, 2018). I used these pre-determined questions to gather and correlate information provided by the participants.

Data Collection Technique

After I received approval from Walden's IRB, approval number 04-24-20-0586342, I conducted interviews to collect the needed information to make a correlation. While a face to face interview provided a chance to build a great rapport versus over the phone, the timing would not permit such an arrangement. Therefore, I conducted the interview via the Zoom virtual call. It helped mimic an in-person interview that helped calm the participant and get better-aligned data to the question. The Zoom meeting, along with the one on one with the participant, assisted in the comfortable presentation of information (Rousseau, Turner, Duncan, O'Cathain, Croot, Yardley, & Hoddinott, 2019). The point of the virtual face-to-face interview was to obtain the information, but also observe body language that helped address any follow-up questions and how to answer those follow-up questions. As with anything, there are some downsides to a face-to-face interview. With a face-to-face interview, the entire process was contingent on the researcher able to comfortably ask the questions and create a comfortable atmosphere for the participant (Castillo-Montoya, 2016). I ensured that the room was comfortable, free of distraction, and I made sure that the participant meets the requirements to participate in the study.

Data Organization Techniques

The collection of data was the focal point in a study. In addition, the organization of that collected data was equally important. The data that I collected was consist of electronic notes, recordings from interviews, and any other data that was collected, all of which were being stored on a secure and encrypted device. BitLocker controlled the encryption key, and the encryption key was stored on a separate device that was password-protected, that only I had access. The information that was collected had a naming convention to help determine the information origin (i.e., O1P1 would indicate Organization 1 and Participant 1). Swygart-Hobaugh (2019) highlights the importance of denoting and coding and making connections amongst the data to assist with alignment. The use of Nvivo was used to help organize the themes throughout the study. Swygart-Hobaugh (2019) found that using Nvivo helps neatly organize the data from a study in a fashion that was accommodating to most that use it. As a side of caution, Atlas.ti was also evaluated to provide a comparison. The use of either data analysis tools was used to orchestrate the information better.

Data Analysis Technique

In addition to the information provided from the participants in the interview, documents shared, industry standards (i.e., NIST Cybersecurity Framework), along with the evaluation of my conceptual framework were used to connect the information and serve as a data source. The documents retrieved from the participants pertained to the policy or some other justification on a course of action to protect the devices or data. To that point, the multiple sources were interviewed, and the information was added to NVivo for tracking and analysis. Clustering took my interview questions, the answers from the participants, along with any documents that are provided and placed them in appropriate clusters that helped with building the themes of the study.

Triangulation

There are a variety of triangulation methods used in research. The methods are data, theory, investigator, and methodological triangulation. All have advantages and disadvantages. The most common one was data triangulation. Data triangulation was the process of using multiple sources to build up the validity of a study (Jentoft & Olsen, 2019). Data triangulation was the method I selected for this study. The data was collected through interviews, artifacts provided, best practices, and industry standards. The other method of triangulation was theory triangulation. In addition, the use of secondary data sources was used. A secondary data source was a source that was published by another person not related to the current study the researcher was conducting (Salkind, 2010).

The secondary sources consisted of NIST frameworks, best practices from the industry, and artifacts presented by the participants. Cater et al. (2014) contends that most researchers conducting qualitative studies collect data by an interview. Also, Carter et al. (2014) stated that the data source triangulation happens best when the collection of the data was from different groups, companies, and communities to ensure that multiple perspectives are met. I collected my data from two different facilities, and each facility had a minimum of three participants. I stopped collecting data when data saturation was met. I knew that data saturation was met with the questions that did not result in any additional information from other participants, and the same conclusion was made.

The theory triangulation method uses a combination of theories to make a connection with the information (Cruz, 2016). The use of theory was used, but a collection of theories was not used to correlate the data or phenomena directly. It was this reason that theory triangulation was not used as the primary triangulation of the study. The other method of triangulation was called the investigator. The use of investigator triangulation was helpful in a study. The concept of investigator triangulation was to provide details from other researchers on a topic (Archibald, 2015). Using this method was very time consuming and would increase the cost of a study (Archibald, 2015). The time restriction was one of the main factors that investigator triangulation was not used in this study (Archibald, 2015). Lastly, methodological triangulation was evaluated for use in the study. The concept of methodological triangulation was the ability to have multiple research methods to gather data or to have one research use multiple research methods (Bryman, 2001). The use of methodological triangulation was beneficial and served its purpose. Still, this study would be time-consuming, and the study was not going to be set up in a manner that other researchers would use the method and data sources.

Reliability and Validity

Reliability and validity work together to align concisely, but an accurate presentation of information in a study (Mohajan, 2017). Mohajan (2017) contends that reliability and validity are two-fold: they both can increase the honesty of the study, as well as decrease the researcher's bias, which could be injected into the study. Spiers et al. (2018) stated that reliability looks at the adequacy of the data and ensures that the data can be used across the participants involved in the study. Just the opposite, validity looks at the felicitousness of the data and provides an accurate reflection of the feedback from the participants (Spiers et al., 2018). In other words, the purpose of reliability and validity in a study was to help the view of the research in a dependable manner. To assist with the reliability and validity of the study, I used member checking after the interviews were conducted. Member checking was a process of validating the data from the researcher and was an accurate reflection of the participant's statement (Birt, Scott, Cavers, Campbell, & Walter, 2016). Member checking or respondent verification (Birt et al., 2016; Creswell & Miller, 2000) was used in this study by collecting the information from the participant, coding the information for theme identification, typing up the information, and presenting it back to the participant the validation. The use of member checking assisted in the dependability and reliability of information by allowing the participant to confirm the information was an accurate reflection of the information they provided (Birt et al., 2016). The participant had a chance to provide feedback on the interpretation. I scheduled a time for the participants to hear and see how the information as interpreted. If needed, additional follow-up interviews were conducted to ensure the information was interpreted accurately. Once the participant confirms the information, then it was added to the NVivo software for further analysis. Naidu and Prose (2018) highlight the opportunity of expanding on the content that helped draw additional conclusions from the participant's answers and therefore validates those answers via member checking.

Aside from member checking, which was critical in the reliability and validity of a study, transferability also serves a vital role. According to Amankwaa (2016), transferability was the process of making the study possible to apply in any setting, situation, and to any group. Lincoln and Guba (1985) also contend that to achieve transferability can be accomplished by using a thick description. The thick description was a method of providing such detail to the phenomena that anyone can use the information to apply in other situations. My study used transferability by describing, in detail, how RAT was able to apply and assist with the creation of appropriate policy surrounding the prevention of malware to IoT. Creswell and Miller (2000) stated that the close relationships that are built with the participants could assist in the validity of the study. The day-in and day-out interaction built on the collaboration that the collection of data through the questioning of their experiences. Another part of reliability and validity was confirmability. Korstjen and Moser (2018) say that confirmability was the process of other researchers being able to confirm the study. The confirmability was vital to show that the information was not a figment of the researcher's imagination (Korstjen & Moser, 2018). One method that can be used in the process to ensure confirmability was met was an audit trail (Korstjen & Moser, 2018). I ensured confirmability by providing detailed information in my notes, recordings, and interactions so that an authorized party can audit it.

The last part to ensure reliability and validity was met was going to be data saturation. Data saturation was the collection of data to the point that no additional information would have an impact on the study, positive or negative (Tran, Porcher, Falissard, & Ravaud, 2016). While it was impossible to remove all bias from a study, the use of member checking, data saturations, and interview protocol can help with such impossibilities (Fusch, Fusch, & Ness, 2017). The data collected through data triangulation combined with data saturation help provide validity in the study (Fusch, Fusch, & Ness, 2017). I kept track of the information provided to be able to identify when data saturation was obtained. I knew that data saturation was reached when information became redundant, and new information was not presented.

Transition and Summary

Section 2 provided a further explanation of the perspective of the study in more detail. Along with the role of the research, I also covered the participants, sampling, and population, and how the study had reliability and validity. Additionally, I outlined how I conducted the research, the methods I decided with, and why. I also identified that NVivo or Atlas.ti could be used for the analysis of the data. To conclude this section, I discussed the reliability and validity of the study and that the two were accomplished through member checking. In Section 3, I discussed the study and its overview, along with the findings from the study.

Section 3: Application to Professional Practice and Implications for Change

In Section 3, I present the findings from the qualitative study, explain and demonstrate the application to professional practices, the implication of social impact, the recommendation for action and further research, and provide my reflection on the study process. I interviewed six participants across two healthcare sites. The interviews were held online with an encrypted Zoom session. I asked the participants questions according to the interview protocol in Appendix B. I was able to identify saturation when the information from all participants at each site met equal responses, and no additional information was found. After each interview, I transcribed the conversation and conducted a second interview where I provided a review of the transcription with the participant. The second interview was the member checking phase. The second meeting allowed the participants to agree or disagree with the information that I transcribed. In addition, I provide a synthesis of the findings, which outlines in more detail in the Presentation of the Findings section.

Overview of Study

The purpose of the study was to find the strategies used to mitigate attacks on medical devices. I used semi-structured interviews, internet calls, and reviewing and analyzing company documents on various topics (e.g., BYOD policy, removable media policy, and similar documents) to collect the data. The core content exists in the Presentation of the Findings, where I discuss the information analyzed from the interviews, correlation to the framework, and the summary of the data. For the ease of reading the findings, I broke down the information in the following way: O = organization and P = was the participant.

Presentation of the Findings

The principal research question was: What strategies do IT security professionals use to prevent malware attacks on IoT medical devices? In the section, I discussed the information found in my research and presented four themes that emerged from the research. I interviewed six participants from two healthcare facilities in Washington, D.C., and Buffalo, N.Y. I conducted all the interviews via Zoom sessions that lasted approximately 30 minutes in length. I recorded and transcribed the meetings. A second interview was conducted to perform member checking to solidify the data triangulation process. The four themes that emerged from the study were: (a) user education to promote security, (b) protection of the environment through layers in security, (c) policy that supports security, and (d) threats that the technical gaps present. The four themes could be used by IT security professionals to help protect their IoT devices from malware attacks. I discovered a holistic strategy used by both facilities. The strategy highlighted a need to understand the environment and its structure, the information and how it is traversing the network, and how a network protects the data. To understand these key points requires an understanding of policy creation and implementation, having multiple layers of security, the gaps that exist and the mitigation, and how the end-user impacts the security.

Theme 1: User Education to Advance Security Initiatives. The first theme that emerged from the analysis of data and transcripts was how each facility educated their users on the importance of cybersecurity. In the study, I used the analysis of the theme which came from six participants from two different organizations to answer the research question: What countermeasures do you have in place to prevent the user of the device from putting the environment at risk of an attack? I used the inquiry highlighted areas that each of the facilities used to ensure the end-users couldn't quickly put the environment at risk. From the analysis of the transcripts and follow-up conversations, I discovered that a pivotal point to the countermeasure was the education of the end-user through a well-structured cybersecurity awareness program.

The structure of the awareness program was essential. According to Mitnick (2017), the information must be presented in such a way that prevents the *prairie dog effect* – where one employee tells another person about the email or fake attack. This effect can minimalize the efforts of the training to take away and decrease the impact of the intention of the program. Likewise, if the program presents relevant fake attacks to areas, a focused effort can be made. For example, if a financial themed false phish attack focuses on a group that does not handle financial records, an assessment of the effectiveness of the program may not be viable (Jensen, Dinger, Wright, & Thatcher, 2017). In addition, NIST SP 800-5, a standards document states,

> Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include, for example, policies,

> procedures, tools, methods, and artifacts for the security and privacy roles defined (Dempsey et al., 2014, p.38).

The need to identify who the training was directed at was critical to the success of a program and adds value to the possible lessons learned. According to the creators of NIST SP 800-50, Wilson and Hash (2003), the structuring of an awareness program can fall in three different models: (a) centralized policy, strategy, and implementation; (b) centralized policy and strategy, distributed implementation; and (c) centralized policy, distributed strategy, and implementation. The main difference between the three models was who constructed the program: all internal personal, mixed constructing with some internal and some external, or all external construction of the program. In all three, the policies are all centralized to the internal team (e.g., the IT security team).

Each of the three has benefits and concerns. For example, if a company went with Model 1, it would be expected that the resources and knowledge came from inside the company, and there was no need for external assistance. If a company selected Model 2, the policy and strategy are internally developed, but implemented by someone else. Lastly, in Model 3, policy creation and maintenance are internal, but everything else was external. It was important to note that at one Model was not any better or worse than another. Rather it depends on the resources available to the facility. If subject matter experts exist internally, and they can support a program, Model 1 may be a good option. The selection of a model aligns well with how an IT security professional can use the Confidentiality, Integrity, and Availability (CIA) triad to protect data, as mentioned in the literature review. The CIA triad focuses on the confidentiality, integrity, and availability of data and the associated risks. Because the end-user can be a risk to the data, a proper method of educating them was necessary to assist in the pursuit to protect data and hardware (Gřivna, & Drápal, 2018; Samonas & Coss, 2014). The information presented to end-users should be formatted in a way that was easy to understand

The cybersecurity awareness program took its unique shape in each of the respected facilities. In each case, users were expected to understand how their actions could impact the overall security of the institution. The selection of how the information was provided to the users appeared to be systematic. The users attended training each year. The training compromised of points from the year and new trends that may surface since the last training. O2P2 stated, "We have annual security training. So, you take not only just regular security training, phishing security, and we do phishing." As noted in the literature, the end-users are closest to the devices and access the information the most. The development of a structured cyber awareness program can positively impact how the end-users view the importance of security (Trim & Lee, 2019).

Both facilities had a cybersecurity awareness model. Compared to the NIST SP 800-50, both facilities would be using a Model 2. It was made evident by the participants that frequent tests got sent to the users. The use of the training, according to O2P2, used benign phishing attacks on the users to see if the training was valid or not. O2P3 stated that,

> We do require an annual Security Awareness Training certification. It's an online step-by-step training for both the awareness of what they're touching, what sort of data they're dealing with, and role-based training. So, we do include that in that

> training, and you must, when you complete it, take a final test on that to get an idea if you are comprehending what the topics.

The importance of comprehension gets repeated throughout the interviews from the participants. O2P1 stated,

> We'll also sat down and educated the end-user. If we knew that the individual opened an infected PDF file, whoever the person was can educate them on recognizing like, and show them telltale signs that this was a malicious attachment.

Structuring training should be needs to make sense to an end-user and was essential to the overall effectiveness of the program. Establishing a sense of ownership to the end-user about the severity of the training was necessary and can change how it was perceived. One key driver in the perception of the training was the support from leaders. O2P3 statement, which paired nicely with O1P2, mentioned that if there was a security breach on a user's device, part of the investigation was to go back and see how that user performed in training. While both participants and organizations used different Models, O2P3 stated,

> We also, after everything has been isolated and taken off the network, do also educate as well on the users. We required them to redo their security awareness training, making sure that they did not just click, click, click to the next screen, and that they understand the severity of what that particular user did do.

Once the user was educated about the circumstance, the expectation was that it was prevented and did not happen again.

In the review of the business document Annual Training Requirements, all end-users must attend annual training online learning modules, and new hires are required to take additional training. Each module serves as a focal point for a specific topic: the first module referred to information security, privacy awareness, records management refresher, and emergency preparedness refresher; the second and third module refered to information security awareness and information management training that all newly hired employees are required to pass. Creating a structured list of training that needs to be complete, the awareness program needs to have support from senior leaders. If the user becomes a habitual offender, there should be a progressive discipline to correct bad behavior. O2P3 stated, "…we also do create a list of if this person was a repeat offender, we might have to follow up with some further notifications, and then their supervisors can decide what the discipline was for them." The aligned approach from IT and leaders about the training may improve the attention that the end-users give to the training.

Maintaining compliance with the program was essential. Having clear expectations can help drive the awareness program to success. Per NIST SP 800-50, an automated tracking system should be used for all the leaders to track the compliance of a program. The compliance provided a better understanding of the gap that may exist in the current state of the company. Reviewing the business document Security Training Website, I found. Also, NIST 800-16 states that all users received specific, including those in management, need to understand the overarching impact of the training (Wilson et al., 1998). The training focused on the roles for each employee. Furthermore, if the user worked remotely then leaders should enforce their employees to get the Secure

Remote Computing training. It would also help to develop the training required that may be specific to a job function. Along with tracking the training of employees and ensuring that users understand their role as it pertains to cybersecurity awareness.

RAT and its modernized offset, Cyber-RAT, aligned well with the theme of user education to advance security initiatives because of the need for capable guardianship or digital guardianship and the totality of victimization. The end-user was under the IT security professional's guardianship when navigating the enterprise and associated networks. If the IT security professional was not able to provide a capable level of guardianship that protects the users from threats, then the user lacks said guardianship. By educating the user about the threats (e.g., phishing attacks), they would improve on their existing knowledge of cybersecurity. The expansion of the knowledge for the end-users closely aligns with the advancement of security initiatives because of the inherent involvement a user has with the data and hardware.

As the literature outlines, the need for a capable guardian is defined in the victim's VIVA. If the victim has high-value information like PHI along with the ease of accessing data and removing it they become prime a target. If the information is stored on a hard drive or they have the rights to access data, the visibility for the offender is increased. If the offender can conceal their identity quickly, and the offender's accessibility to the victim is. Under the premise of RAT, the lack of capable guardianship were the most crucial aspect when evaluating the reduction of victimization of users (Leukfeldt & Yar, 2016).

Table 1

User education to advance security initiatives

Source of data collection	D
Participants	6
Industry Standardization Documents	2
Business Documents	3

Note. Theme 1, user education to advance security initiatives; *D*= data collected from.

Theme 2: Protection of the Infrastructure Through Layered Security

The second theme that emerged from the study was the protection of the infrastructure through layered security. The theme was developed while analyzing provided documents, transcripts, and follow-up meetings with the participants. All participants from both facilities aligned with this theme as a critical part of the overarching security posture. While the layered security appeared different at each facility, the overall approach remained the same. The protection of infrastructure through layered security was a multifaceted concept that takes various topics and views them holistically. Some of the topics used for this theme overlapped into other themes in the study. There were three topics that participants addressed in the interviews that were also found in the documents shared: (a) asset control, (b) encryption, and (c) network security

Asset Control. Part of the layered strategy started with understanding what assets existing in the environment. O2P1 stated, "All of our devices go to our property management section where they get inventoried, barcoded, and labeled." O1P1 stated, "There's a couple of different tools. We run the traditional MDM technology, or your mobile devices, like the iPhones; there are Android-based devices as well, that was on our network that provides, that we use in a hospital setting that was managed. We also have laptops that we manage around the network." Understanding the assets in an environment as part of the initial understanding of what needs to be protected (Cadler, 2018). The ability to track a device was important, but so was knowing what can join your network. Creating a list of devices that can join the network, also known as whitelisting, can limit what rogue devices are allowed on the network. Mendez and Yang (2018) stated that whitelisting a device can control what information can reach a device, and if a device can connect at all. The use of whitelisting adds another level of management for the devices. As mentioned by O1P1, "…workstations that are making connections physically on our network, go to a central correlator such as SIEM." Having an insight on who and what was connected to a network was a critical point, especially when an IT security professional was attempting to control assets (Díaz López et al., 2018).

In the evaluation of business documents Mobile Device Policy, Medical Device Computers SLA, and IT Medical Device Computers SOP, it was found that the use of asset tracking software was required and in use. As the Mobile Device Policy highlights, "…furnished mobile devices must be enrolled in this MDM service before allowing direct access to IT resources." The MDM protocol allows the user(s) to access information from O2 applications to perform job functions and provide access for IT security professionals to monitor the devices if needed. Also, the Medical Device Computers SLA pressed the importance of updating the devices and keeping a schedule,

"…weekly software updates with the Department POC. The computer updated through weekly software "pushes." These included updates to the OS and applications such as Java, Adobe, .Net, etc. Remediation of security vulnerabilities was coordinated with the Department POC." The use of a schedule appears to place accountability for the device and those using the device. Deviation from the updates schedule must be submitted to the CIO with an explanation, again establishing accountability and further control of the asset.

Encryption. If the data and hardware can be isolated in a manner that prevents the attacker from accessing either, then it adds a layer to the environment (Schaumont & Montuschi, 2018). During the review of the business document Encryption Policy, I found that each structure had a detailed policy. The file server, desktop, laptop, and other mobile storage devices carried a specific guideline. The policy stated, "Users are not authorized to copy data from government-furnished equipment (GFE) to non-GFE," which highlights a clear indication that users can't take data from encrypted devices to non-encrypted devices. In addition, any USB thumb drive had to be approved by a designated IT representative. Furthermore, data loss prevention (DLP) technology was used to help monitor the compliance of data to and from GFE.

One form of isolation was encryption. O2P1 indicated "…data in transit, all of that has to be encrypted as well so again. We use encryption methods like TLS 1.2 or above since 1.0 and 1.1 are not deprecated, to ensure that all the traffic from our services, for our IoT devices, primarily medical devices in this case, to the actual laboratory information system are encrypted. Then for data in motion, that's hard for RAM. Still, we do also do, for our databases, we also enable encryption at the bottom level to ensure that if there's any PII or PHI, that information was encrypted as well." A similar mindset was shared by O1P2 when it came to removable media (e.g., USB jump drives). "On a USB, it forced it to be encrypted because we're not going to block activity. Of course, it was encrypted; we'll record it." As mentioned in the literature, encryption intends to keep the information protected from those not the reviewers of that data.

Network Security. Securing a network is more than just authenticating with a username and a password. IT security professionals can use a filtration tool or technique (e.g., MAC filtering or Cisco Umbrella) to assist in tracking rouge devices added to the network unbeknownst to the IT security professional. During my review of the business document Information Security Report stated that "High risks allow malicious parties to easily gain access to the network, compromising sensitive information and valuable data. These risks can be identified through vulnerability scanning, penetration testing, or evaluation of a system's architecture and security controls." As noted by O2P1, "…before it's [the device] released to the end-user, our user support team was responsible for registering the MAC address of that device in our MAC tool, so we ensure that this was an authorized device on the network." The use of MAC filtering speaks to the literature that references providing access to only authorized devices to the network and capturing the assets on the network. Al-Moshaigeh, Dickins, and Higgs (2019) highlighted that also, the hardware could be paired with what type of data that resided on the device. The two attributes, data and asset awareness, provides a higher level of awareness on the network and establishes accountability.

Along with knowing the location of the asset and the data that resides, being able to segment based on the information provides or device was an additional layer of network security. O1P2 highlights, "…we segment access for them within medical devices. We have a whole separate segment that was just ID pumps. There's a lot of segmentation." The network segmentation aligns with network security by layering the data and devices in the network through multiple layers, commonly referred to as "Defense in Depth" or DiD. DiD is a concept that takes a security structure and layers the defenses available such that if one layer were hindered, it wouldn't jeopardize the infrastructure. Mansfield-Devine (2016) highlights that the challenges are knowing what devices are on the network to protect. Therefore, the practice of network security is more than a firewall, Intrusion Detection and Prevention Systems, and antivirus. It prevents the attacker from accessing your environment with multiple protection and not having a failure point to exploit.

An example of weak network security came from the evaluation of the business document Penetration Testing Report. While a secure network passed the annual penetration test, it was discovered that some of the configurations needed adjustments. In this example, a user's device could have strong security, password, and physical access. Still, a weak configuration of the network could provide an attack via a graphic user interface to the public and provide a vector of attack (e.g., brute-force) to the administrative interface. While these findings were fixed, it is essential to the point that this was a single point of failure, could be used to gain access to vital interfaces and attack infrastructure.

During my review of the business document Pen Test Remediation Process, I discovered that the testing was conducted by an internal team that carried out a methodical approach. The Internal Vulnerability Assessment (VA) was completed in four phases: discovery, detection, exploitation, and analysis/recommendations. Each phase owned a specific step and required various teams to perform tasks. For example, during the discovery phase, all entry point into the facilities network was evaluated. The required some assistance from the IT staff, CISO, and CIO to ensure that all entry points were found.

The development of this theme partnered well with the RAT—specifically, a suitable target. Providing ways to prevent attackers from accessing an infrastructure takes away the potential for a business or person to appear to be a suitable target. As mentioned in the literature, there are four attributes of a suitable target: value, inertia, visibility, and access. When an attacker looks for a victim(s), the value, whether monetary or other means, is considered; in the case of an IoT device, the known lightened security and antivirus methods can be exploited. But placing the IoT devices in an air-gapped or secluded VLAN can improve the exploitation of the same device. Also, access to the attacker had an impact on who would be attacked. If an attacker can perform a scan of a network and find IoT devices, the attacker knows what can and can't be exploited. Hiding these devices is a layer that can be considered. With both attributes in mind, IT security professionals can look at how to protect an environment in layers. If a layer is hindered, it will not give access to the attacker, and an attack can potentially be mitigated.

Table 2

Protection of the Infrastructure Through Layered Security

Source of data collection	D
Participants	6
Business Documents	5

Note. Theme 2, Protection of the Infrastructure Through Layered Security; *D*= data collected from.

Theme 3: Policy that supports security

Policies that support the technical needs provides substance to the purpose and, therefore, includes consistency for enforcement when needed—the evaluation of transcripts from both organizations and industry standards. The use of the policy was demonstrated, and the support of senior leaders was made clear. The first finding of this support was with O2P1, who mentioned, "…procurement strategy in terms of, you can't buy certain devices from certain companies like Huawei to other requirements like, the vendor must be able to identify supply chain management and also identify any supply chain threats." The vetting process of who the company could use for the procurement of machines was a policy that was enforced. The enforcement of the policy was also supported by not just the senior leaders but also by other departments, as demonstrated by the option to order from other unapproved vendors.

Likewise, O2P3 stated, "…in the end, it's the executive who needs to go ahead and accept the risk on all of this [security of the infrastructure]. Knowing the executive leadership was involved helps provide more authority to the process." The statement from O2P3 also aligned with O1P1, who said, "The policy process in general at O2 was very structured. Part of that was due to not only the regulatory nature of health care but also because we do have a union representation throughout the facilities and the system. In terms of information security, policies are initially drafted or developed primarily within my team. And it'll go through peer review before being brought to the operational policy council." O1P1 provides some additional insight as to how the variety of reviews helps the process shape the variety of groups it would apply to when published. The use of the policy in a real scenario was addressed by O2P3, who stated, "we do lean on our processes and procedures that we do have in place. So, it would require technology to limit the device. We have an incident response checklist that we go through, where we involve executives at the executive level, as well as subject matter experts, both at the server level and the network level, where we immediately activate a call on our end here, which means that a conference call was kicked off." The involvement of an executive team or member helps the situation by providing more authority to a situation and promotes additional involvement of other departments. As Elmiligi et al. (2016) highlighted, providing a policy to a specific framework or approach helps solidify an approach and establishes consistency.

In my analysis of the organizational document SOP Index, I discovered the organization document Encryption Policy. I discovered that the oversight of the policy carried not just at the mid-level of a manager or director but also at the executive level. The policy explains the minimum requirements for encryption, but also outlines if encryption was not possible, that other security measures must be utilized. The policy continues to explain how the movement of data was monitored, "A Data Loss Prevention

(DLP) system/tool must be implemented to monitor and prevent loss of sensitive data. The DLP tool shall perform frequent scans regularly to ensure sensitive information was stored and protected in compliance with policies." The development of the process for encryption also used best practices from NIST 800-111, which also outlines that having the storage was not enough. Access to the data must also be access-controlled (Scarfone et al., 2007). The Encryption Policy shows the additional protection by indicating that access must be requested from a responsible person (e.g., Information Security Officer, ISO).

The organizational document Mobile Device Policy identifies that mobile devices pertain to several devices. The changing of the devices, the ability of those devices, and the interconnect ability presents some issues with a static policy. Therefore, updating the policy needs to occur due to the changing of technology and common trends. As O1P2 indicated, "we review them on a biannual basis, although we're trying to look to move to an annual basis with them. And really, it's becoming more of a mature program." Looking at a process from an objective manner helps place the policy on an omnidirectional path, which means that the policy was applied to all parties that share a common usage (e.g., billing department or HR using a technology). Because multiple departments comprise an organization, it was sometimes helpful to include a standard operating procedure that ties in a policy. During the review and analysis of the industry standardization document NIST 800-124 (Souppaya & Scarfone, 2013), the overarching list of applications that aren't allowed establishes a baseline for all users. According to O2P3, "It helps to have some sort of standard operating procedure for a lot of processes that tend to repeat itself, tend to be repetitive. Anything did annually, quarterly, as far as timeframes are concerned, it makes it easier to create standard operating procedures or SOPs as we call them."

RAT aligns with the policy that supports the security theme because if any of the three attributes of RAT are missing (motivated offender, a suitable target, and absence of a guardian), then a criminal act was likely (Cohen & Felson, 1979). The use and enforcement of policy provide guardianship. The criminal uses areas of opportunity, and the lack of policy can provide an opening that promotes individual situations that presents a security risk. For example, if a company does not have a policy about social media usage or picture taking in the workplace, then the potential for someone to post a picture that reveals sensitive information can be enough for an attacker to offend. The policy itself was not the guardian; rather, it was the leaders that enforce the policy that serves as the guardian. Likewise, having the policy was an administrative control that helps enforce the controls. While the policy itself does not prevent misuse, it does support the disciplinary action of a violation that could put the data at risk. Therefore, the support structure of a policy combined with appropriate actions that can take place prevents no or poor security control.

Table 3

Third Theme

Source of data collected	D
Participants	6
Industry Standardization Documents	2
Business Documents	3

Note. Theme 3, policy that supports security; *D*= data collected from.

Theme 4: Threats that the technical gaps present

Identifying the gaps in an assessment was important. The lack of attention to the gaps can present a significant security concern. The best method of figuring out the gaps was to have an annual assessment of the infrastructure from an unbiased third party. Also, to maintain the infrastructure, having a way to conduct vulnerability scans help on an ongoing basis. O1P1 stated, "We have begun to move toward increased vulnerability scanning of these devices. We are moving towards increased logging of their activity, and we're in the market right now for more advanced medical devices and security equipment." Understanding the gap, as O1P1 stated, provides a clear and actionable task to prevent potential attacks.

Being able to address the gaps was important, but strategizing the resolution was also helpful in ensuring all facets of solutions. O2P1 stated, "We have what's known as a security and technical board meeting every Monday. At that meeting was where the security team presents all the vulnerabilities within our organization to all the different stakeholders. Then we get updates in terms of where are you on patching all high or critical vulnerabilities, are you experiencing any challenges, obviously one of the major challenges that we face was that we're a medical organization as well, so a lot of times out technical points of contact are waiting on the vendor to give the go-ahead that you can apply x, y, z patch before they release into production." According to the FIPS 199 standard, having and understanding the potential impact an organization has and what would be needed to remediate any risks was paramount in the threat assessment process (NIST, 2004).

The evaluation of company policies and industry standards NIST 800.37 and 800.53B, outlines that being proactive and systemic with safeguarding technologies. The policies and standards also allow for technology and sometimes a user to lower concern of performing a function or task that would place infrastructure in jeopardy. An idea was shared that providing the users a method to visit non-business websites while on break could help with the urge to access. This idea was highlighted by O1P1, being proactive and eliminating the potential of personal internet searches or other non-business-related topics can be prevented. O1P1 goes on to say, "We also look to satisfy various free time, various satisfiers. People do have downtime, they do take breaks, and they may want to go shopping, for example, during the workday or their break. We have accessible guest Wi-Fi that associates can use. It was on our network, but it's segregated. And there was a less restrictive firewall policy in place that allows some of that behavior. Individuals are allowed to bring them. We do have the BYOD policy." Providing the option to allow users to search helps prevent the urge to do so in a more protected environment. In the analysis of the policy, it was evident that other departments supported the policy. It was referenced in the HR onboarding process and reinforced by the annual training required for all to watch and pass the given quiz.

There were other common concerns— the use of honeypots and lack of staffing. A honeypot was a technical diversion tactic that takes the attention of the attacker to a fake environment, as opposed to a live production environment. O2P1 said, "Honeypots are something that if we had time, we would look into, doing it internally for our organization, but since obviously, the challenge for us was that we're short of staff, was that we have to do more of a so we do try to maximize our tools to the best of our abilities." As the literature shows, honeypots can be helpful in 'holding' the attacker's attention, and therefore possibly diverting their attention away from production data.

Du and Wang (2019) highlight that the use of intrusion detection systems has many resource requirements and can consume in the trillions of bytes per second. By leveraging honeypots, the traffic would be minimal because it was only capturing data from sources that are pretending to be legitimate. Therefore, pretending resources can consume the time and resources of the attacker (Du & Wang, 2020). Furthermore, the use of honeypots was not a 'fix-all' approach and be optimized using additional honeypots, known as a pseudo-honeypot game or "PHG" (Du & Wang, 2020). The collection of honeypots deployed served as decoys for the attackers and would likely not consume as much as an IDS but trick the attackers even further.

Also, O2P1 refers to staffing issues that prevented the use of honeypots. Wirth (2017) highlighted that, even though the healthcare IT staffing in 2016 increased to 11%, staffing and budget were still large barriers in getting the right people to use the right application to protect infrastructure. Wirth (2017) also commented that the IT security leader needed to set a proper expectation to the board of directors that sustains adequate staffing and budget.

RAT aligns with the threats that the technical gaps present theme as it denotes the possibility of a lack of guardianship and makes facilities a suitable target. Cohen and

Felson (1979) stated if there were a motivated offender, a suitable target, and a lack of guardianship, a crime could occur. Defining these gaps helps with the alignment of areas of opportunities that a criminal may exploit. The ability to divert the attackers away from critical information while draining the resources decreases the motivation the offender would have initially. Likewise, if the staffing levels of the IT security team are improved, the lack of guardianship is removed as well. The staffing resources are used to monitor and proactively address concerns more efficiently. Hence, providing a heightened level of guardianship to the infrastructure.

Table 4

Threats that the technical gaps present

Source of data collected	D
Participants	6
Industry Standardization Documents	3
Business Documents	1

Note. Theme 4, threats that the technical gaps present; *D*= data collected from.

Applications to Professional Practice

The information provided in the findings has the potential to provide insight into IT security professionals on how to protect medical devices from malware attacks. The protection of medical devices provides security to the data and to the patient. The information in this study could be used to prevent malware attacks that could jeopardize the safety of both the patient and data. To say that an environment will never be attacked is not logical, and the mindset of such can prove to be detrimental. The lack of a strategic approach for protecting medical devices can place a hospital and its devices at risk for an attack. The IT security professional should try to take an unbiased view of the current infrastructure for the gaps to be identified. Obtaining feedback from a third-party vendor helps assure; there is no bias. The use of technology is to assist medical professionals to perform their jobs more effectively and provide the best outcomes for the patient. If the data can't abide by confidentiality, integrity, and availability guidelines, then the use of that information would not be helpful to the medical professionals and could cause irreversible damages to the patient.

Implications for Social Change

The findings of this study may help IT security professionals protect their IoT devices from malware and other attacks. The medical devices are sometimes critical for medical professionals to provide accurate and helpful assessments to the patients. The attack of a medical device can be financially devasting to a healthcare facility, decrease the public trust for the healthcare facility, and cause death from the attackers altering automatic dosage calculation or altering the power output. If the IT security professional chooses not to implement a strategy to protect data, ramifications from governing bodies could ensue, fines from a vendor or other agencies, and much more as a result of improper protections that are required. It may be important for senior IT security leaders to evaluate their environment using these strategies—to ensure that the critical parts of protecting IoT are met. While this list was not all-inclusive of all steps needed to protect a multifaceted environment, it does outline the strategies that could be used to protect IoT devices against malware attacks. From the findings of this study, IT security professionals can apply these strategies to strengthen network security, heighten awareness to end-user about the part they play in cybersecurity, engage senior IT security leaders in purposeful conversation about using a policy that supports the security, and address the technical gaps that present threats.

Recommendations for Action

In this study, I looked for the strategies that IT security professionals used to protect IoT devices from malware attacks. The findings demonstrated that a strategy needs to be layered and not have a single direction approach (e.g., only implementing encryption). The strategy needs to be adopted by security professionals and owned by all levels of management. The strategy required resources to develop or maintain the environment along with a dedicated budget that aligns tools and hardware with best practices that improve the security posture. Most importantly, a steadfast commitment to enforcing the needed changes to improve any deficiencies. Senior IT security leaders must understand that these strategies are not just reading material, but rather a way to approach security. The use of IoT devices continues to increase as technology advances. Not having a strategy to protect the devices and the information increases the likelihood of an attack.

Because the use of cybersecurity best practices was an ongoing process, the IT security leaders need to have a peer-reviewed improvement methodology. The review can assist in the best practices that are or aren't being used and provide an unbiased assessment of the current practices. The peer-review should meet at a regularly scheduled time (e.g., once a month), and that meeting should have clear agendas on what was covered. Lastly, there was the importance of the IT security professional to adopt a way to measure success. There are multiple methods to do this but starting out with a baseline was critical. Understanding the uptime of the network, standardization of configuration, clear processes that help outline all steps, and establishing a service level agreement was a good start.

I am looking to create a summary for all the participants that are interested in having one. I also want to create a version of the study that can be sent to journals for publishing. It was my goal to get this information to as many professionals as possible to help bridge any gaps that exist.

Recommendations for Further Study

In this multiple case study, I conducted semistructured interviews that looked at what strategies IT security professionals were using to protect IoT devices from malware attacks. The study was focused on the healthcare environment, but I can see this expanding to any industry and having it apply to any device, not just IoT. An additional focus can be around the reason existing strategies are used, and if they are effective or not. I also think that using other states would present a different outlook. The regulations may change from state to state and therefore change the strategy. I requested multiple participants, but I was only able to get six participants. The number of participants still allowed for data saturation to occur, but more perspectives could lead to additional themes. Lastly, the specific details of the hardware and technology used can provide more insight and reasoning for a specific strategy. The focus of this study was to look at a strategy and how it protected IoT devices. I think a deeper dive into the use of the existing technology can be leveraged to provide a more specific focus on IoT.

Reflections

This study was an eye-opening experience. The last two and a half years have been filled with a lot of ups and downs. I can say that my perspective on things changed about three times during the study. I was also humbled along the way. I improved my patience during the process and was able to take in, sometimes hard to hear, constructive criticism. I am incredibly thankful for the time I spent on this study and with the people that assisted me along the way. I knew that when I started this journey, it would be a long process.

When I started with the study, I was told to find something that I enjoyed studying, as I would be stuck to that topic. I know now that the topic of "A Secure and Strategic Approach to Keep IoT Devices Safe from Malware Attack" was a good decision. When I selected the topic, I knew that IoT, specifically medical devices, would be a good focus, and the Mid-Spring of 2017 proved that even more. Mid-Spring of 2017 was when a large-scale international attack called WannaCry reared its ugly head. While it did not focus on IoT; specifically, it did highlight the lack of patch management, which was a tenant of this study.

The process taught me the importance of information gathering, analytical perspectives, and being unbiased. During my research, I read over 150+ articles about the subject matter and the theoretical approach. I was able to take those articles and use them to create a solid foundation for the study. Lastly, because the interviews were semistructured, I had to be certain not to inject my own bias on a statement or topic from the participants and did so to the best of my ability.

Summary and Study Conclusions

The development of a strategy for protecting IoT devices was not a clear-cut process. There needs to be a collaborative effort on both ends of the equation. The senior leaders need to understand that the risk of not having a strategy to protect IoT device was equally important to any other device. Likewise, IT security professionals need to understand that having a strategy was not a single point solution, meaning it was layered with other technologies and concepts. Learning from past mistakes and other facilities that have dealt with attacks was important to develop or adjust a strategy.

If there was a need to implement new policies or technologies that impact the end-users, the leadership needs to help drive the message and support the direction of the IT security professionals. While the leadership and IT security professionals make the changes, it was equally important that the users are listened to for any issues or concerns that are brought up. During the change, it was recommended that a 'town hall' style meeting was set up to address any concerns from the staff. The meeting needs to be a listening exercise for the leadership and IT teams. As facilities mature in the strategic approach, it was important to review policies and procedures constantly. Looking at the strategy, adjusting to new trends, and seeking better processes and technologies was an ongoing journey that must be met with consistency and good leadership.

References

Aldosari, H., Snasel, V., & Abraham, A. (2016). A novel security layer for Internet of things. *Journal of Information Assurance & Security*, *11*(2), 58-66. Retrieved from http://www.mirlabs.org/jias

Al-Moshaigeh, A., Dickins, D., & Higgs, J. L. (2019). Cybersecurity Risks and Controls. *CPA Journal, 89*(6), 36–41.

Amankwaa, L. (2016). Creating Protocols for Trustworthiness in Qualitative Research. *Journal of cultural diversity, 23*(3), 121–127.

Aminzade, M. (2018). Confidentiality, integrity and availability – finding a balanced IT framework. *Network Security*, *2018*(5), 9-11. doi:10.1016/s1353-4858(18)30043-6

Anderson, C. A., Leahy, M. J., DelValle, R., Sherman, S., & Tansey, T. N. (2018). Methodological application of multiple case study design using modified consensual qualitative research (CQR) analysis to identify best practices and organizational factors in the public rehabilitation program. Journal of Vocational Rehabilitation, 41(2), 87-98. doi:10.3233/jvr-140709

Anderson, R. (2018). Making Security Sustainable. *Communications of the ACM*, *61*(3), 24–26. doi:10.1145/3180485

Anggorojati, B., & Prasad, R. (2018). Securing communication in the IoT-based health care systems. *Jurnal Ilmu Komputer dan Informasi*, *11*(1), 1. Retrieved from https://doi.org/10.21609/jiki.v11i1.562

Archibald, M. M. (2015). Investigator Triangulation: A Collaborative Strategy with Potential for Mixed Methods Research. *JOURNAL OF MIXED METHODS RESEARCH, 10*(3), 228–250. doi:10.1177/1558689815570092

Arias, O., Wurm, J., Hoang, K., & Jin, Y. (2015). Privacy and Security in Internet of Things and Wearable Devices. *IEEE Transactions on Multi-Scale Computing Systems*, *1*(2), 99–109. doi:10.1109/tmscs.2015.2498605

Arias-Gómez, J., Villasís-Keever, M., & Miranda-Novales, M. (2016). The research protocol III. Study population. *Revista Alergia México, (2)*, 201. doi: 10.29262/ram.v63i2.181

Arshad, S., Azam, M., Rehmani, M., & Loo, J. (2019). Recent Advances in Information-Centric Networking-Based Internet of Things (ICN-IoT). *IEEE Internet of Things Journal, 6*(2), 2128-2158. doi:10.1109/jiot.2018.2873343

Ashwood, F., Vanguelova, E., Benham, S., & Butt, K. (2019). Developing a systematic sampling method for earthworms in and around deadwood. *Forest Ecosystems, (1),* 1. doi:10.1186/s40663-019-0193-z

Badenhorst, C. (2018). Citation Practices of Postgraduate Students Writing Literature Reviews. *London Review of Education, 16*(10), 121-135. Retrieved from doi:10.18546/lre.16.1.11

Baillette, P., Barlette, Y., & Leclercq-Vandelannoitte, A. (2018). Bring your own device in organizations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end users. *International Journal of Information Management, 43*, 76–84. doi:10.1016/j.ijinfomgt.2018.07.007

Belanger, F., & Crossler, R. (2018). Dealing with digital traces: Understanding protective behaviors on mobile devices. *The Journal of Strategic Information Systems*. *28* (1), 34-49 (2018) doi:10.1016/j.jsis.2018.11.002

Beresford, A., Mascolo, C., & Gruteser, M. (2018). The Specter of Malicious Computing: Securing the Internet of Things. *IEEE Pervasive Computing, 17*(3), 10-11. doi:10.1109/mprv.2018.03367730

Bergmann, C., Dreißigacker, A., von Skarczinski, B., & Wollinger, R. (2018). Cyber-Dependent Crime Victimization: The Same Risk for Everyone? CyberPsychology, Behavior & Social Networking, 21(2), 84–90. Retrieved from https://doi.org/10.1089/cyber.2016.0727

Bertino, E., Choo, K., Georgakopolous, D., & Nepal, S. (2016). Internet of things (IoT). *ACM Transactions on Internet Technology*, *16*(4), 1-7. Retrieved from https://doi.org/10.1145/3013520

Biros, M. (2018). Capacity, Vulnerability, and Informed Consent for Research. Journal of Law, *Medicine & Ethics, 46*(1), 72–78. Retrieved from https://doi.org/10.1177/1073110518766021

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member Checking: A Tool to Enhance Trustworthiness or Merely a Nod to Validation? *QUALITATIVE HEALTH RESEARCH, 26*(13), 1802–1811. doi: 10.1177/1049732316654870

Bock, K., Shannon, S., Movahedi, Y., & Cukier, M. (2017). Application of Routine Activity Theory to Cyber Intrusion Location and Time. European Dependable Computing Conference (EDCC). doi: 10.1109/EDCC.2017.24

Bransen, J. (2001). Philosophy of International Encyclopedia of the Social & Behavioral Sciences, 16165-16170. doi:10.1016/b0-08-043076-7/01022-6

Bryman, A. (2001). Content Analysis. In *Social Research Methods*. New York, NY: Oxford University Press, USA.

Burns, A. J., & Johnson, M. E. (2015). Securing Health Information. *IT Professional, 17*(1), 23–29. https://doi.org/10.1109/mitp.2015.13

Busse, C., Kach, A., & Wagner, S. (2016). Boundary conditions: What they are, how to explore them, why we need them, and when to consider them. *Organizational Research Methods*, *20*(4), 1-36. doi: 10.1177/1094428116641191

Cakmak, Z., & Akgün, H. (2017). A theoretical perspective on the case study method. *Journal of Education and Learning*, *7*(1), 96-102. doi:10.5539/jel.v7n1p96

Calder, A. (2018). NIST Cybersecurity Framework. doi:10.2307/j.ctv4cbhfx

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014). The Use of Triangulation in Qualitative Research. *Oncology Nursing Forum, 41*(5), 545–547. doi:10.1188/14.onf.545-547

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *Qualitative Report*, 21, 811-831. Retrieved from http://nsuworks.nova.edu/cgi/viewcontent.cgi?article=2337&context=tqr

Chalee, V., Soontorn, S., Ekkachan, R., & Visut, S. (2017). A Policy-Based Framework for Preserving Confidentiality in BYOD Environments: A Review of Information Security Perspectives. *Security and Communication Networks*, (2017). doi:10.1057/978-1-137-53585-6_2

Charman, A. J., Petersen, L. M., Piper, L. E., Liedeman, R., & Legg, T. (2016). Small Area Census Approach to Measure the Township Informal Economy in South Africa. *Journal of Mixed Methods Research*, *11*(1), 36-58. doi:10.1177/1558689815572024

Chatfield, T., & Reddick, G. (2018). A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government. Government Information Quarterly. doi:10.1016/j.giq.2018.09.007

Cho, S., Jang, D., & LoCascio, S. (2016). Is Simple Random Sampling Better than Quota Sampling? An Analysis Based on the Sampling Methods of Three Surveys in South Korea. *Asian Journal for Public Opinion Research, (4),* 156. doi:10.15206/ajpor.2016.3.4.156

Cho, V., & Ip, W. H. (2018). A Study of BYOD adoption from the lens of threat and coping appraisal of its security policy. *Enterprise Information Systems, 12*(6), 659–673. doi:10.1080/17517575.2017.1404132

Choi, K. (2008). Cyber-Routine Activities: Empirical Examination of Online Lifestyle, Digital Guardians and Computer-Crime Victimization. *Cyber Criminology*, (pp. 229-252) CRC Press. doi:10.1201/b10718-19

Choi, K., Earl, K., Lee, J., & Cho, S. (2018a). Diagnosis of cyber and non-physical bullying victimization: A lifestyles and routine activities theory approach to constructing effective preventative measures. *Computers in Human Behavior, 92*, 11-19. doi:10.1016/j.chb.2018.10.014

Cohen, E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review. 44*(4): 588–608. doi:10.2307/2094589

Cohen, I., & Mello, M. (2018). HIPAA and Protecting Health Information in the 21st Century. *JAMA, The Journal of the American Medical Association, (3),* 231. Retrieved from doi:10.1001/jama.2018.5630

Cornish, D., & Clarke, R. (1986). Understanding Crime Displacement: An Application of Rational Choice Theory. *Criminology, 25*(4), 933-948. doi:10.1111/j.1745-9125.1987.tb00826.x

Cox, G. (2019). Managing the risks of shadow IoT. Network Security, 2019 (1), 14–17. doi:10.1016/s1353-4858(19)30010-8

Creswell, J. W., & Miller, D. L. (2000). Determining Validity in Qualitative Inquiry. *Theory Into Practice*, *39*(3), 124-130. doi:10.1207/s15430421tip3903_2

Cruz, A. (2016). On the Job: White Employers, Workers of Color, and Racial Triangulation Theory. *On the Job. Sociology Compass, 10*(10)*,* 918-927. doi:10.1111/soc4.12406

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers & Security, 48*, 281–297. doi:10.1016/j.cose.2014.11.002

Dempsey, K., Chawla, S., Johnson, A., Johnston, R., Jones, C., Orebaugh, D., & Stine, M. (2011). Information Security Continuous Monitoring (ISCM) for federal information systems and organizations. doi:10.6028/nist.sp.800-137

Dempsey, K., Witte, G., & Rike, D. (2014). Summary of NIST SP 800-53 revision 4, security and privacy controls for federal information systems and organizations. https://doi.org/10.6028/nist.cswp.02192014

Dennis, C. (2018). Why is patch management necessary? *Network Security, 7*, 9–13. doi:10.1016/s1353-4858(18)30068-0

Díaz López, D., Blanco Uribe, M., Santiago Cely, C., Vega Torres, A., Moreno Guataquira, N., Morón Castro, S., & Gómez Mármol, F. (2018). Shielding IoT against Cyber-Attacks: An Event-Based Approach Using SIEM. *Wireless Communications & Mobile Computing*, 1–18. doi:10.1155/2018/3029638

Dorogovs, P. (2016). E-service security challenges: Availability, integrity, confidentiality. *Baltic Journal of Modern Computing, 4*(1), 68-78. Retrieved from https://ezp.waldenulibrary.org/login?url=https://search-proquest-com.ezp.waldenulibrary.org/docview/1785390994?accountid=14872

Du, M., & Wang, K. (2020). An SDN-enabled pseudo-honeypot strategy for distributed denial of service attacks in industrial Internet of things. *IEEE Transactions on Industrial Informatics*, *16*(1), 648-657. doi:10.1109/tii.2019.2917912

Ducich, S., & Fischer, J. (2018). The General Data Protection Regulation: What U.S.-Based Companies Need to Know. *Business Lawyer, 74*(1), 205–215. Retrieved from https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=bth&AN=134947820&site=eds-live&scope=site

Dysart, J. (2018). Quantum Computing: The End of Encryption? *Communications of the ACM*, *61*(5), 28. Retrieved from https://ezp.waldenulibrary.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=129270735&site=eds-live&scope=site

Ebert, C., & Dubey, A. (2019). Convergence of Enterprise IT and Embedded Systems. *IEEE Software, 36*(3), 92-97. doi:10.1109/ms.2019.2896508

Ellouze, N., Rekhis, S., Boudriga, N., & Allouche, M. (2018). Powerless security for Cardiac Implantable Medical Devices: Use of Wireless Identification and Sensing Platform. *Journal of Network and Computer Applications*, *107*, 1-21. doi:10.1016/j.jnca.2018.01.009

Elmiligi, H., Gebali, F., & El-Kharashi, M. W. (2016). Multi-dimensional analysis of embedded systems security. *Microprocessors and Microsystems, 41*, 29–36. doi:10.1016/j.micpro.2015.12.005

Elnaggar, R., & Chakrabarty, K. (2018). Machine Learning for Hardware Security: Opportunities and Risks. *Journal of Electronic Testing, 34*, 183-201.

Engeström, Y. (2018). The Future of Activity Theory: A Rough Draft. *Learning and Expanding with Activity Theory*, 303-328. doi:10.1017/cbo9780511809989.020

Erdem, Ö., Pektaş, A., & Kara, M. (2018). HoneyThing: A New Honeypot Design for CPE Devices. *KSII Transactions on Internet & Information Systems, 12*(9), 4512–4526. Retrieved from https://doi-org.ezp.waldenulibrary.org/10.3837/tiis.2018.09.021

Feigelson, J., Jim, P., Serrato, K., & Jonathan, M. (2016). New Federal Guidance on Cybersecurity for Mobile Devices. *Intellectual Property & Technology Law Journal*, 28(3), 25-26

Felson, M., & Clarke, R. (1998). Opportunity makes the thief: practical theory for crime prevention. Retrieved from https://popcenter.asu.edu/sites/default/files/opportunity_makes_the_thief.pdf

Fu, K., & Xu, W. (2018). Risks of Trusting the Physics of Sensors: Protecting the Internet of Things with embedded security. *Communications of the ACM*, *61*(2), 20–23. doi:10.1145/3176402

Fusch, I., & Ness, R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report, 20*(9), 1408-1416. Retrieved from http://www.nova.edu/ssss/QR/QR20/9/fusch1.pdf

Fusch, P. I., Fusch, G. E., & Ness, L. R. (2017). How to conduct a mini-ethnographic case study: A guide for novice researchers. *Qualitative Report, 22*(3), 923-941. Retrieved from http://nsuworks.nova.edu/tqr/vol22/iss3/16

Gönültas, B., Oral, G., & Beyaztas, G. (2015). Examining theories describing sexual abuse in the context of criminal investigations/Cinsel istismarları açıklayan teorilerin suç soruşturmaları bağlamında irdelenmesi. *Journal of the Justice Academy of Turkey/Türkiye Adalet Akademisi Dergisi, 6*(21):79-104. Retrieved from https://www.ncjrs.gov/pdffiles1/ovw/241903.pdf

Gonzalez-Manzano, L., De Fuentes, J. M., & Ribagorda, A. (2019). Leveraging User-related Internet of Things for Continuous Authentication: A Survey. *ACM*

Computing Surveys, 52(3), 1–38. Retrieved from https://doi-org.ezp.waldenulibrary.org/10.1145/3314023

Grable, J., & Lyons, C. (2018a). An Introduction to Big Data. *Journal of Financial Service Professionals*, *72*(5), 17–20. Retrieved from https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=bth&AN=131378067&site=eds-live&scope=site

Gřivna, T., & Drápal, J. (2018). Attacks on the confidentiality, integrity and availability of data and computer systems in the criminal case law of the Czech Republic. *Digital Investigation, 28*, 1–13. doi:10.1016/j.diin.2018.12.002

Guerar, M., Merlo, A., Migliardi, M., & Palmieri, F. (2018). Invisible CAPPCHA: A usable mechanism to distinguish between malware and humans on the mobile IoT. *Computers & Security*, *78*, 255-266. doi:10.1016/j.cose.2018.06.007

Guri, M., & Elovici, Y. (2018). Bridgeware: The Air-Gap Malware. *Communications of the ACM, 61*(4), 74–82. Retrieved from https://doi-org.ezp.waldenulibrary.org/10.1145/3177230

Hawdon, J., Costello, M., Ratliff, T., Hall, L., & Middleton, J. (2017). Conflict Management Styles and Cybervictimization: Extending Routine Activity Theory. *Sociological Spectrum, 37*(4), 250-266. doi:10.1080/02732173.2017.1334608

He, S., Cheng, B., Wang, H., Huang, Y., & Chen, J. (2017). Proactive personalized services through fog-cloud computing in large-scale IoT-based healthcare application. *China Communications*, *14*(11), 1-16. doi:10.1109/cc.2017.8233646

Health Insurance Portability and Accountability Act of 1996 (HIPAA). (2019, February 21). Retrieved from https://www.cdc.gov/phlp/publications/topic/hipaa.html

Hoffman, L., & Novak, P. (2018). Consumer and Object Experience in the Internet of Things: An Assemblage Theory Approach. *Journal of Consumer Research, 44*(6), 1178-1204. doi:10.1093/jcr/ucx105

Hollis, E., Felson, M., & Welsh, C. (2013). The capable guardian in routine activities theory: A theoretical and conceptual reappraisal. *Crime Prevention and Community Safety, 15*(1), 65–79. doi:10.1057/cpcs.2012.14

Hollis-Peel, E., & Welsh, C. (2014). What makes a guardian capable? A test of guardianship in action. *Security Journal, 27*(3), 320. doi:10.1057/sj.2012.32

Hossain, M., Islam, S. R., Ali, F., Kwak, K., & Hasan, R. (2018). An Internet of Things-based health prescription assistant and its security system design. *Future Generation Computer Systems, 82*, 422-439. doi:10.1016/j.future.2017.11.020

Hosseinabadi, R., Karampourian, A., Beiranvand, S., & Pournia, Y. (2013). The effect of quality circles on job satisfaction and quality of work-life of staff in emergency 125 medical services. International Emergency Nursing, 21(4), 264-270. doi:10.1016/j.ienj.2012.10.002

Hoyme, K. (2017). Future Directions in Healthcare Systems Engineering. *Biomedical Instrumentation & Technology, 51*(3), 206-207. doi:10.2345/0899-8205-51.3.206

Iannarelli, J., & O’Shaughnessy, M. (2015). The Threats of Today and Tomorrow. Information Governance and Security, 13-27. doi:10.1016/b978-0-12-800247-6.00002-9

Jacobson, I., Spence, I., & Ng, P. (2017). Is there a single method for the internet of things? *Communications of the ACM, 60*(11), 46–53. doi:10.1145/3106637

Jacobson, M., Brackbill, R., Frazier, P., & Gargano, L. (2019). Conducting a study to assess the long-term impacts of injury after 9/11: participation, recall, and description. *Injury Epidemiology, (1)*, 1. doi:10.1186/s40621-019-0186-y

Jang, J., Jung, I., & Park, J. (2016a). An effective handling of secure data stream in IoT. *Applied Soft Computing, (68)*, 811–820. doi:10.1016/j.asoc.2017.05.020

Jarrett, P. (2017). Cybersecurity-A Serious Patient Care Concern. JAMA: *Journal of The American Medical Association, 318*(14), 1319. doi:10.1001/jama.2017.11986

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, *34*(2), 597-626. doi:10.1080/07421222.2017.1334499

Jentoft, N., & Olsen, T. S. (2019). Against the flow in data collection: How data triangulation combined with a “slow” interview technique enriches data. *Qualitative Social Work, 18*(2), 179–193. doi:10.1177/1473325017712581gio

Kaivo-oja, J. (2017). Towards better participatory processes in technology foresight: How to link participatory foresight research to the methodological machinery of qualitative research and phenomenology?. *Futures, 86*, 94-106. doi: 10.1016/j.futures.2016.07.004

Ka Man, L., Mei Na, C., & Chun Kit, N. (2015). IoT-Based Asset Management System for Healthcare-Related Industries. *International Journal of Engineering Business*

Management. Retrieved from https://doi-org.ezp.waldenulibrary.org/10.5772/61821

Keese, J., & Motzo, L. (2005). Proactive approach to malware for healthcare information and imaging systems. *International Congress Series, 12*(81), 943-947. doi:10.1016/j.ics.2005.03.326

Khan, M., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems, 82*, 395-411. doi:10.1016/j.future.2017.11.022

Kohout, J., Komárek, T., Čech, P., Bodnár, J., & Lokoč, J. (2018). Learning communication patterns for malware discovery in HTTPs data. Expert Systems with Applications, 101, 129–142. doi:10.1016/j.eswa.2018.02.010

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22,* 113–122. doi:10.1016/j.jisa.2014.09.005

Lakhoua, N. (2019). Review on Smart Hospital Management System Technologies. *Research and Science Today, 1*, 187-194.

Leclercq - Vandelannoitte, A. (2015). Managing BYOD: how do organizations incorporate user-driven IT innovations?, *Information Technology & People, 28*(1), 2-33, Retrieved from https://doi.org/10.1108/ITP-11-2012-0129

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263-280. doi:10.1080/01639625.2015.1012409

Lips-Wiersma, M., & Mills, A. J. (2014). Understanding the basic assumptions about human nature in workplace spirituality: Beyond the critical versus positive divide. *Journal of Management Inquiry, 23*, 148-161. doi:10.1177/1056492613501227

Magruder, J., Lewis, S., Burks, E., & Smolinski, C. (2015). Bring Your Own Device (BYOD)--Who Is Running Organizations? *Journal of Accounting & Financ*e, *15*(1), 55–61. Retrieved from https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=bth&AN=115755815&site=eds-live&scope=site

Majhi, S., Patra, G., & Dhal, S. (2016). Cyber physical systems & public utility in India: State of art. *Procedia Computer Science, 78*, 777-781. doi:10.1016/j.procs.2016.02.052

McCallister, E., Grance, T., & Scarfone, A. (2010a). Guide to protecting the confidentiality of Personally Identifiable Information (PII). doi:10.6028/nist.sp.800-122

Meister, L. (2018). On methodology: How mixed methods research can contribute to translation studies. *Translation Studies, 11*(1), 66–83. doi:10.1080/14781700.2017.1374206

Mendoza, C., & Kleinschmidt, J. (2015). Mitigating On-Off Attacks in the Internet of Things Using a Distributed Trust Management Scheme. *International Journal of Distributed Sensor Networks*, *11*(11), 859731. doi:10.1155/2015/859731

Middaugh, D. J. (2016). Nursing Management. Do Security Flaws Put Your Patients' Health at Risk?. *MEDSURG Nursing, 25*(2), 131-132.

Ming-Li, H., & Shun-Yung, K. (2018). Routine Activities in a Virtual Space: A Taiwanese Case of an ATM Hacking Spree. International Journal of Cyber Criminology, 333–352. Retrieved from https://doi-org.ezp.waldenulibrary.org/10.5281/zenodo.1467935

Mitnick, K. (2017). A History of Cyber Security Attacks, (pp. 3-10) Auerbach Publications. doi:10.1201/9781315155852-2

Mohajan, H. (2017). Two Criteria for Good Measurements in Research: Validity and Reliability. Annals of Spiru Haret University Economic Series, (4), 59. doi:10.26458/1746

Moos, J. (2017). IoT, Malware and Security. *Itnow*, *59*(1), 28-29. doi:10.1093/itnow/bwx013

Morris, N., Armstrong, V., & Balmer, B. (2009). Constructing a safe research environment: technology talk between researchers and volunteer research subjects. *Health, Risk & Society, 11*(2), 99–116. doi:10.1080/13698570902784299

Morse, M., & Niehaus, L. (2016). *Mixed method design: Principles and procedures*.

Muslukhov, I., Sun, S.-T., Wijesekera, P., Boshmaf, Y., & Beznosov, K. (2016). Decoupling data-at-rest encryption and smartphone locking with wearable devices. Pervasive and Mobile Computing, 32, 26–34. doi:10.1016/j.pmcj.2016.06.016

Naidu, T., & Prose, N. (2018). Re-Envisioning Member Checking and Communicating Results as Accountability Practice in Qualitative Research: A South African

Community-Based Organization Example. *Forum: Qualitative Social Research*, (3). Retrieved from https://doi-org.ezp.waldenulibrary.org/10.17169/fqs-19.3.3153

Nayyar, A., & Puri, V. (2016). Data Glove: Internet of Things (IoT) Based Smart Wearable Gadget. *British Journal of Mathematics & Computer Science, 15*(5), 1–12. doi:10.9734/bjmcs/2016/24854

Nieles, M., Dempsey, K., & Pillitteri, V. (2017). An introduction to information security. doi:10.6028/nist.sp.800-12r1

Nikitkov, A. N., Stone, D. N., & Miller, T. C. (2014). Internal Controls, Routine Activity Theory (RAT), and Sustained Online Auction Deception: A Longitudinal Analysis. *Journal of Information Systems, 28*(1), 311–337. doi:10.2308/isys-50708

Nikolopoulos, D., & Polenakis, I. (2017). Preventing malware pandemics in mobile devices by establishing response-time bounds. *Journal of Information Security and Applications, 37*, 1–14. doi:10.1016/j.jisa.2017.09.002

NIST. (2004). *Standards for security categorization of federal information and information systems*. NIST Computer Security Resource Center CSRC. Retrieved from https://doi.org/10.6028/nist.fips.199

Owens, B. (2016). Stronger rules needed for medical device cybersecurity. *The Lancet*, *387*(10026), 13-64. doi:10.1016/ s0140-6736(16)30120-9

Özdemir, P., Tanhan, F., & Özdemir, O. (2018). Rational Choice Theory in Psychiatry. *Current Approaches in Psychiatry / Psikiyatride Guncel Yaklasimlar, 10*(4), 484–495. Retrieved from https://doi-org.ezp.waldenulibrary.org/10.18863/pgy.362157

Park, J., & Park, M. (2016). Qualitative versus Quantitative Research Methods: Discovery or Justification? *Journal of Marketing Thought, 3*(1), 1–7. Retrieved from https://doi-org.ezp.waldenulibrary.org/10.15577/jmt.2016.03.01.1

Pauwels, J., Svensson, R., & Hirtenlehner, H. (2018). Testing Situational Action Theory: A narrative review of studies published between 2006 and 2015. *European Journal of Criminology*, *15*(1), 32-55. doi:10.1177/1477370817732185

Peterson, J. (2019). Presenting a Qualitative Study: A Reviewer's Perspective. *Gifted Child Quarterly, 63*(3), 147–158. Retrieved from https://doi.org/10.1177/0016986219844789

Pishva, D. (2017). IoT: Their Conveniences, Security Challenges and Possible Solutions. Advances in Science, Technology and Engineering Systems Journal, 2(3), 1211-1217. doi:10.25046/aj0203153

Pratt, T., & Turanovic, J. (2016). Lifestyle and Routine Activity Theories Revisited: The Importance of "Risk" to the Study of Victimization. *Victims & Offenders, 11*(3), 335–354. Retrieve from https://doi-org.ezp.waldenulibrary.org/10.1080/15564886.2015.1057351

Reyns, B., Henson, B., & Fisher, B. (2018). Being Pursued Online. *Criminal Justice and Behavior*, *38*(11), 1149-1169. doi:10.1177/0093854811421448

Reyns, B., Henson, B., Fisher, B., Fox, K., & Nobles, M. (2015). A Gendered Lifestyle-Routine Activity Approach to Explaining Stalking Victimization in Canada. *Journal of Interpersonal Violence, 31*(9), 1719-1743. doi:10.1177/0886260515569066

Rghioui, A., & Oumnad, A. (2017). Internet of Things: Surveys for Measuring Human Activities from Everywhere. *International Journal of Electrical and Computer Engineering (IJECE)*, *7*(5), 24-74. doi:10.11591/ijece.v7i5.pp2474-2482

Ripley, A. (2010). Is Cash the Answer? Time, (15). Retrieved from https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=edsgea&AN=edsgcl.246479802&site=eds-live&scope=site

Rutberg, S., & Bouikidis, D. (2018). Exploring the Evidence. Focusing on the fundamentals: a simplistic differentiation between qualitative and quantitative research. *Nephrology Nursing Journal, 45*(2), 209-213. Retrieved from https://ezp.waldenulibrary.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=129106232&site=eds-live&scope=site

Salkind, N. J. (2010). *Encyclopedia of research design* Thousand Oaks, CA: SAGE Publications, Inc. doi: 10.4135/9781412961288

Samonas, S., & Coss, D. (2014). The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security. *Journal of Information System Security*, *10*(3), 21.Retrieved from http://www.proso.com/dl/Samonas.pdf

Sampson, F., Goodacre, S., & O' Cathain, A. (2019). The Reality of Pain Scoring in the Emergency Department: Findings from a Multiple Case Study Design. *Annals of Emergency Medicine, 74*(4), 538–548. Retrieved from https://doi-org.ezp.waldenulibrary.org/10.1016/j.annemergmed.2019.02.018

Schaefer, L., & Mazerolle, L. (2017). Putting process into routine activity theory: Variations in the control of crime opportunities. *Security Journal, 30*(1), 266-289. Retrieved from http://dx.doi.org.ezp.waldenulibrary.org/10.1057/sj.2015.39

Schaumont, P., & Montuschi, P. (2018). The Rise of Hardware Security in Computer Architectures. *IEEE Computer, 51*, 4-5.

Schnell, C., Grossman, L., & Braga, A. (2018). The routine activities of violent crime places: A retrospective case-control study of crime opportunities on street segments. Journal of Criminal Justice. https://doi-org.ezp.waldenulibrary.org/10.1016/j.jcrimjus.2018.10.002

Sha, K., Wei, W., Yang, T., Wang, Z., & Shi, W. (2018). On security challenges and open issues in Internet of Things. *Future Generation Computer Systems, 83*, 326–337. doi:10.1016/j.future.2018.01.059

Shukla, S. (2019). Editorial: Distributed Public Ledgers and Block Chains-What Good Are They for Embedded Systems? *ACM Transactions on Embedded Computing Systems, 16*(1). Retrieved from https://doi-org.ezp.waldenulibrary.org/10.1145/3001902

Signes-Pont, M. T., Cortés-Castillo, A., Mora-Mora, H., & Szymanski, J. (2018). Modelling the malware propagation in mobile computer devices. *Computers &*

Security, *79*, 80–93. Retrieved from https://doi-org.ezp.waldenulibrary.org/10.1016/j.cose.2018.08.004

Soma, J., Courson, J., & Cadkin, J. (2009). Corporate privacy trend: the “value” of personally identifiable information ('PII’) equals the “value” of financial assets. *Richmond Journal of Law & Technology (Online), (4)*, 1. Retrieved from https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=edsglt&AN=edsgcl.227477341&site=eds-live&scope=site

Sosin, A. (2018). How to Increase the Information Assurance in the Information Age. *Journal of Defense Resources Management, 1*(45). Retrieved from https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=edsdoj&AN=edsdoj.2dbbd0cb37444c0fb51d3df6d5c24cf5&site=eds-live&scope=site

Stapleton, J. (2019). Spoofing a Hardware Security Module. *ISSA Journal, 17*(1), 24-30. Retrieved from https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct+true&db=tsh&AN=133951375&site=eds-live&scope=site

Sung, Y. (2019). Cyber-Sexual Violence Victimization of College Women Students: Test of Cyber Lifestyle-Routine Activity Theory. *Korean Association of Criminal Psychology*, *15*(1), 89-104. doi:10.25277/kcpr.2019.15.1.89

Surmiak, A. (2019). Should we Maintain or Break Confidentiality? The Choices Made by Social Researchers in the Context of Law Violation and Harm. *Journal of Academic Ethics*. doi:10.1007/s10805-019-09336-2

Thomas, J., Silverman, S., & Nelson, J. (2015). *Research Methods in Physical Activity 7th Edition* (7th ed.).

Tong, C. (2006). Refinement strategies for stratified sampling methods. Reliability Engineering and System Safety, 91(10), 1257–1265. Retrieved from https://doi-org.ezp.waldenulibrary.org/10.1016/j.ress.2005.11.027

Tran, V.-T., Porcher, R., Falissard, B., & Ravaud, P. (2016). Point of data saturation was assessed using resampling methods in a survey with open-ended questions. *Journal of Clinical Epidemiology, 80*, 88–96 doi:10.1016/j.jclinepi.2016.07.014

Trim, P. R., & Lee, Y. (2019). The role of B2B marketers in increasing cyber security awareness and influencing behavioral change. *Industrial Marketing Management*, *83*, 224-238. doi:10.1016/j.indmarman.2019.04.003

United States Department of Health and Human Services. (1979). The Belmont report. Retrieved from http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html

Uribeetxebarria, A., Martínez-Casasnovas, J. A., Escolà, A., Rosell-Polo, J. R., & Arnó, J. (2019). Stratified sampling in fruit orchards using cluster-based ancillary information maps: a comparative analysis to improve yield and quality estimates. *Precision Agriculture, 20*(2), 179–192. doi:10.1007/s11119-018-9619-9

Van Ouytsel, J., Ponnet, K., & Walrave, M. (2016). Cyber Dating Abuse Victimization Among Secondary School Students from a Lifestyle-Routine Activities Theory

Perspective. *Journal of Interpersonal Violence*, *33*(17), 2767-2776. doi:10.1177/0886260516629390

Vasileiou, K., Barnett, J., Thorpe, S., & Young, T. (2018). Characterizing and justifying sample size sufficiency in interview-based studies: systematic analysis of qualitative health research over 15 years. *BMC Medical Research Methodology, 18*(1), 148. doi:10.1186/s12874-018-0594-7

Weber, R. (2015). The digital future – A challenge for privacy? *Computer Law & Security Review, 31*(2), 234–242. doi:10.1016/j.clsr.2015.01.003

Weller, S., Vickers, B., Bernard, H., Blackburn, A., Borgatti, S., Gravlee, C., & Johnson, J. C. (2018). Open-ended interview questions and saturation. *PLOS ONE, 13*(6). doi:10.1371/journal.pone.0198606

Wencheng, S., Zhiping, C., Yangyang, L., Fang, L., Shengqun, F., & Guoyan, W. (2018). Security and Privacy in the Medical Internet of Things: A Review. *Security and Communication Networks*, doi:10.1155/2018/5978636

Whitman, E., & Mattord, J. (2018). Principles of information security. Boston, MA: Cengage Learning.

Wick, S., Nagoshi, C., Basham, R., Jordan, C., Kim, Y., Nguyen, A., & Lehmann, P. (2017). Patterns of Cyber Harassment and Perpetration among College Students in the United States: A Test of Routine Activities Theory. *International Journal of Cyber Criminology, 11*(1), 24–38. Retrieved from https://doi-org.ezp.waldenulibrary.org/10.5281/zenodo.495770

Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. doi:10.6028/nist.sp.800-50

Wirth, A. (2017). The Economics of Cybersecurity. Biomedical Instrumentation & Technology: Cyber Vigilance: Keeping Healthcare Technology Safe and Secure in a Connected World, Vol. 51, No. s6, p. 55-59. doi.org/10.2345/0899-8205-51.s6.52

Xu, J., Yao, J., Wang, L., Ming, Z., Wu, K., & Chen, L. (2018). Narrowband Internet of Things: Evolutions, Technologies, and Open Issues. *IEEE Internet of Things Journal, 5*(3), 1449-1462. doi:10.1109/jiot.2017.2783374

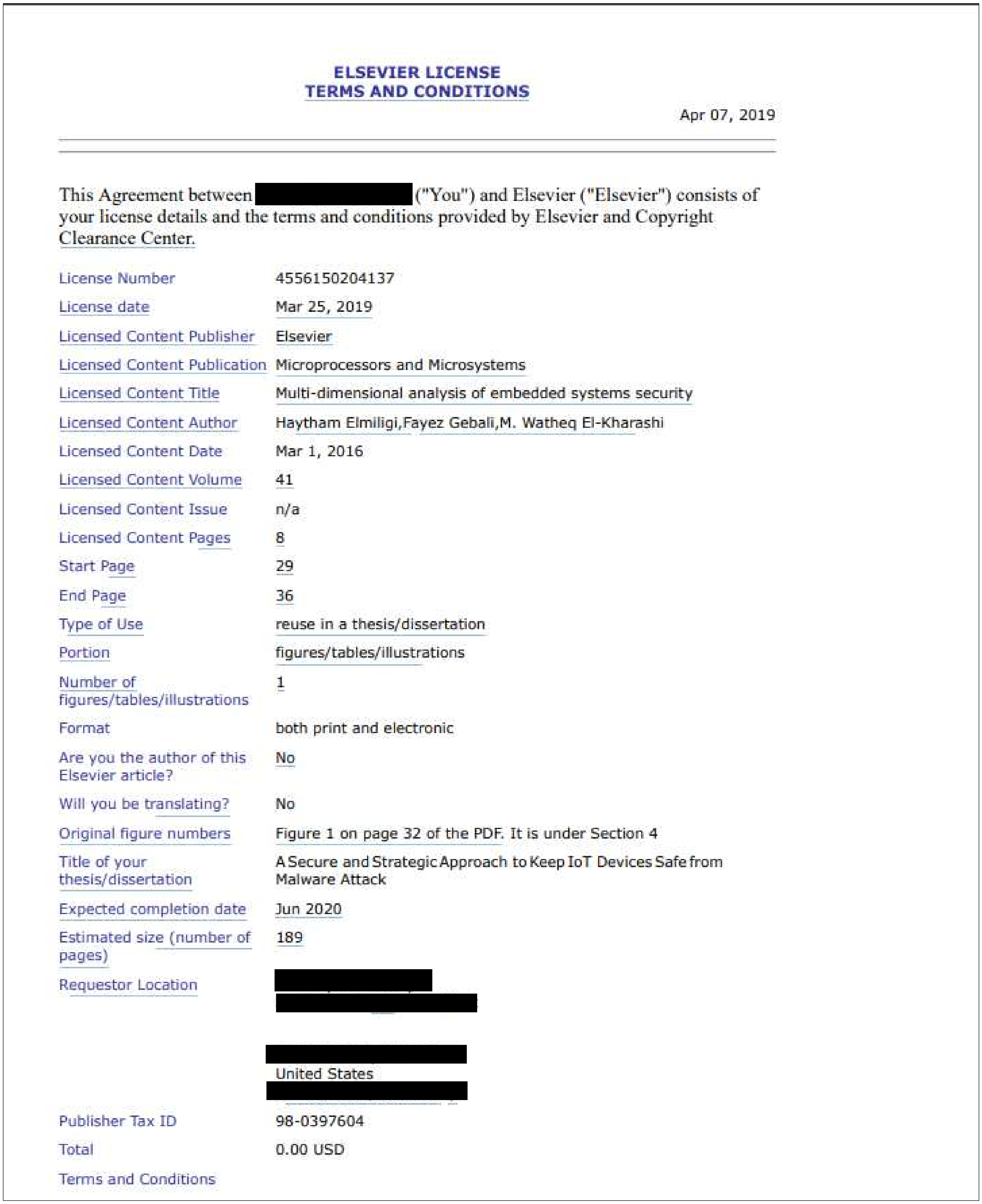
Xuequn, W., Wang, A., & Heiko, G. (2017). Factors driving employee participation in corporate BYOD programs: A cross-national comparison from the perspective of future employees. *Australasian Journal of Information Systems, 21*. doi:10.3127/ajis.v21i0.1488

Yang, Y., Zheng, X., & Tang, C. (2017). Lightweight distributed secure data management system for health internet of things. *Journal of Network and Computer Applications, 89*, 26–37. doi:10.1016/j.jnca.2016.11.017

Yi, C., & Cai, J. (2019). A Truthful Mechanism for Scheduling Delay-Constrained Wireless Transmissions in IoT-Based Healthcare Networks. *IEEE Transactions on Wireless Communications*, *18*(2), 912-925. doi:10.1109/twc.2018.2886255

Yin, R. (2014). Case Study Research Design and Methods (5th ed.). Thousand Oaks, CA: Sage. 282 pages. Retrieved from https://doi-10.3138/cjpe.30.1.108

Appendix A: Copyright Permission



ELSEVIER LICENSE
TERMS AND CONDITIONS

Apr 07, 2019

This Agreement between [redacted] ("You") and Elsevier ("Elsevier") consists of your license details and the terms and conditions provided by Elsevier and Copyright Clearance Center.

License Number	4556150204137
License date	Mar 25, 2019
Licensed Content Publisher	Elsevier
Licensed Content Publication	Microprocessors and Microsystems
Licensed Content Title	Multi-dimensional analysis of embedded systems security
Licensed Content Author	Haytham Elmiligi,Fayez Gebali,M. Watheq El-Kharashi
Licensed Content Date	Mar 1, 2016
Licensed Content Volume	41
Licensed Content Issue	n/a
Licensed Content Pages	8
Start Page	29
End Page	36
Type of Use	reuse in a thesis/dissertation
Portion	figures/tables/illustrations
Number of figures/tables/illustrations	1
Format	both print and electronic
Are you the author of this Elsevier article?	No
Will you be translating?	No
Original figure numbers	Figure 1 on page 32 of the PDF. It is under Section 4
Title of your thesis/dissertation	A Secure and Strategic Approach to Keep IoT Devices Safe from Malware Attack
Expected completion date	Jun 2020
Estimated size (number of pages)	189
Requestor Location	[redacted] [redacted] United States [redacted]
Publisher Tax ID	98-0397604
Total	0.00 USD
Terms and Conditions	

Appendix B: Interview Protocol

1. Introduce myself, the study and thank the participant.
2. Confirm all questions have been answered about the consent form and ensure the consent form is received.
3. Explain the process of the interview, inform the participant that it will be recorded and that all information is strictly confidential.
4. Begin the recording on the device and identify who the participant is with an identifier (i.e., Participant 1) along with the date and time.
5. Begin the interview with the first question and continue until there are no more questions. Allow the participant to answer and ask questions.
    a. How long have you worked at your company?
    b. What is your position and role in the company?
    c. How many years’ experience do you have in cybersecurity?
    d. What degrees or certifications do you possess?
    e. Please describe the strategies you are utilizing to prevent attacks on IoT medical devices. What part did you play in the plan?
    f. How are you preventing the activities that motivate an offender to want to attack an IoT device?
    g. What countermeasures do you have in place to prevent the user of the device from putting the environment at risk of an attack?
    h. What is your current strategy for protecting data that may reside on an IoT device?

i. What is your process for responding to an attacked device? Has this process been tested? If, so how often and in what scenario?

j. Is there a process for the policy to be created? If so, what is your role in the process approval?

6. Allow the participant to provide any clarifying statements or additional information about the topic.
7. Ask if there is any documentation that would be relevant or helpful to any topics discussed.
8. Inform the participant about member checking and that there will be a follow-up interview to clarify the recording of their answers.
9. Stop the recording device.
10. Thank the participant for the interview and provide my contact information.

Appendix C: Invitation Letter

Dear [name of participant],

My name is Christopher Murray. I am a Doctor of Information (DIT) student at Walden University. I am performing research on what strategies are used to protect IoT devices, specifically medical devices. The overall research question I am looking to address is: What strategies do IT security professionals use to prevent malware attacks on IoT medical devices?

The information that is provided in this interview will be kept confidential. I have included a consent form for you to review and sign before the interview is conducted. The consent form will provide you with some background and explain your rights during the interview process.

Based on your experience in cybersecurity, I would like to interview you to obtain some insight into how [facility name] mitigates cyber threats on IoT devices. The interview will take 30-45 minutes of your time and will be scheduled within the next two weeks at a time and place that is most convenient for you. It would be helpful for you to provide any documentation, reports, or audits that will help outline the strategy used to mitigate threats to IoT devices. If you can provide documents, it will be at your discretion and will not impact your participation in the interview.

If you have any questions or concerns, please find the best method of contacting me in my signature below. If you can participate, I will ask for an email response indicating your participation. Once I receive Walden IRB approval, I will kindly contact you to schedule an interview. Thank you again for your support of my study and your consideration.