2022

Strategies for the Reduction of Cybersecurity Breaches in Hospitals

Donovan M. A. Pottinger
Walden University

Walden University

College of Management and Human Potential

This is to certify that the doctoral study by

Donovan M. A. Pottinger

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. Gail Miles, Committee Member, Information Technology Faculty
Dr. Gary Griffith, University Reviewer, Information Technology Faculty

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

Walden University
2022

Abstract

Strategies for the Reduction of Cybersecurity Breaches in Hospitals

by

Donovan M. A. Pottinger

MS, Andrews University, 1992

MA, Andrews University, 1988

BA, Northern Caribbean University, 1980

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

August 2022

Abstract

Recent cyberattacks in hospitals show the urgency of the need to enhance secure information technology (IT) infrastructure. Hospitals are statistically more at cyber risk than all the multiple industries against ransomware, malware, hacking and internal threats. Guided by routine activity theory, the purpose of this exploratory multiple case study was to explore strategies utilized by hospitals' IT security managers to reduce cybersecurity breaches associated with sensitive data. The participants were nine IT security managers from hospitals in the eastern United States. Data were collected via semistructured interviews and supporting documentation from the consenting participants and hospitals' websites. Through thematic analysis, seven core themes emerged: (a) ensure adherence to top cybersecurity framework, (b) implement adequate and effective cybersecurity controls, (c) conduct a regular cybersecurity risk assessment, (d) maintain an air gap technique backup, (e) cultivate security awareness culture, (f) encrypt all data at rest and in transit, and (g) keep abreast with cybersecurity news and risks. A key recommendation for IT security managers is to utilize the maintenance of regularly updated backup as a crucial tactic for reducing exposure to cybercriminals. The implication for positive social change includes the potential to increase patients' trust and reduce the threat to human life.

Strategies for the Reduction of Cybersecurity Breaches in Hospitals

by

Donovan M. A. Pottinger

MS, Andrews University, 1992

MA, Andrews University, 1988

BA, Northern Caribbean University, 1980

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

August 2022

Dedication

Far transcending human imagination are the supreme beings through the presence of the unseen supernatural being, in the person of the Holy Spirit, to whom I devote this doctoral study. In the realm of humanity, I dedicate this dissertation study to the love of my life, Dr. Sonia Brown-Pottinger, who stood by me in this long and demanding doctoral marathon. Your constant encouragement, support, and belief in my abilities helped me muster the strength and vitality to accomplish this remarkable achievement. My mother, who believes I am the most educated offspring, she shares with the rest of the world, Mrs. Hazel McNeil-Crooks; my sister Mrs. Lorna Dunkley and other siblings; my brilliant sons, Don A. Pottinger and Darren A. Pottinger; and my close friends and relative who were great supporters. I will forever be thankful for the support, prayers, encouragement, and patience in completing my doctoral study.

Acknowledgments

The journey to becoming a doctor was not without help, support, and guidance from notable persons along my path to completion. To my doctoral chairs and mentors, Dr. Christos Makrigeorgis (posthumously), Dr. Steven Case, and Dr. Jon Mckeeby, I am genuinely thankful for the exceptional guidance and support provided me through the entire odyssey. Even through the challenging times, they demonstrated support and encouraged me to perform to the best of my God-given abilities to be successful. Your hard work to see me succeed to the point of graduation is deeply appreciated. To my committee members, Dr. Gail Miles and Dr. Gary Griffith, thank you for the scholarly contributions and exceptional guidance in producing a high-quality dissertation. I am thankful to Mrs. Chevelisia Farmer, who encouraged me to ask permission to pursue this study. I am also grateful to the person who initially approved my request, Mr. Derek Manley. I express my profound gratitude to every Walden University student, especially Dr. Cody Taylor, and the faculty who helped create an exceptional milieu for sharing knowledge and experiences and fostering follow-up relationships. I am incredibly thankful to everyone who participated in this research to contribute solid expertise to the field of study, information technology, and the neighborhood's social welfare. Finally, I give eternal thanks to Jesus, who gave me the inherent abilities to complete this exceptional milestone. I believe in the presence of the Holy Spirit, who empowered me to use this opportunity to His name, honor, and glory.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

Cybersecurity became a significant focus for hospital facilities in the 2010s due to prominent data breaches. Hospital facilities are increasingly vulnerable to recent cybersecurity attacks due to both increasing frequency of such attacks and their increased sophistication. The main reasons why hospitals are targeted are that they do not keep abreast with new and evolving cyber threats (Kruse et al., 2017) and the fact that data theft has potential monetary rewards. In general, data breaches pose not only monetary losses, but also breaches in customer trust and severe harm in relationships with current and future patients. In the remainder of this section, I will address the background of the problem and the purpose of the study.

Background of the Problem

Cybersecurity is a foremost concern for governments and private organizations such as hospitals around the world (Cavelty, 2014). The primary concern of a hospital involves how to protect itself against cyberattacks. Likewise, technological cyber attackers manipulate weaknesses to steal information with monetary value from hospitals. Although hackers continue to produce sophisticated attack vectors, hospital leaders are puzzled as to what strategies to use for defense while providing exceptional patient and customer care. One of the most devastating attack vectors on hospitals is ransomware, which quadrupled in 2020 (Morgan, 2017). Furthermore, Ginni Rometty, IBM Corp Chairman and Chief Executive Officer, stated in 2016 that cybercrime is the top threat to every company in the world (Arcuri et al., 2017). Consequently, the Global State of Information Security® Survey 2016 from Price Waterhouse Coopers stated that 57% of

the public sector necessitates workforces to complete training in privacy policies to address data-privacy initiatives (Coopers, 2017) proactively. Thus, hospitals do not keep up with hackers and are in urgent need of improvement of protection.

Protection against the cyberattack risks on hospitals depends on the strength of the triad pillars of cybersecurity: confidentiality, availability, and integrity. Therefore, in this study, it was fitting to focus on the breaches and threats that can unsettle the information security of hospitals' sensitive data (Lošonczi et al., 2016). Cybersecurity implementation in hospitals guards against sustained risks from hackers who might capitalize on unauthorized access to sensitive information by exploiting vulnerabilities found in the security infrastructure (Rathi & Parmar, 2015). Consequently, in this study, I explored the phenomenon of strategies that information technology (IT) security managers put in place to reduce cybersecurity breaches in hospitals.

Problem Statement

Deep, sustained, and multipronged cyberattacks on hospitals' information security are having damaging effects on core hospital operations and causing irreversible damage to consumers (Gordon et al., 2017). According to the U.S. Department of Health and Human Services (2015), breaches of protected health information (PHI) involving at least 500 consumers or more had increased in 2014 by 12% from 2013 and by 30% from 2012. Such data indicate escalating risk rates for attacks. The general IT problem is that health institutions are an increasing target for cybercriminals, especially because health data comprise sensitive personally identifiable and priced monetary information. The specific

IT problem is that some hospital IT security managers lack security strategies to reduce cybersecurity breaches associated with sensitive data.

Purpose Statement

The purpose of this qualitative, multiple-case study was to explore the strategies utilized by hospital IT security managers to reduce cybersecurity breaches associated with sensitive data. The research population consisted of IT security managers from three medium-sized hospitals in the eastern region of the United States with cybersecurity strategies to protect against breaches associated with sensitive data. The conclusions from this study may benefit information security practice by increasing the overall understanding of the complex nature of internal and external threats and breaches and the strategies utilized to combat such threats. Consequently, as a result of increased protection of users' private data, the findings from this study may contribute to positive social change by reducing patient concerns related to potential identity theft.

Nature of the Study

For this research, I considered quantitative and mixed methodologies. However, such methodologies would have been less constructive to the complete aspirations of this study for several reasons. A quantitative interrogator constructs the foundation of positivist epistemology, where researchers utilize theory to create and examine hypotheses (Everett et al., 2015). The formulation and testing of hypotheses were not the aim of this study. The pragmatism philosophy forms the basis of mixed-methods research. Mixed-methods research involves integrating two complementary approaches, qualitative and quantitative (Onwuegbuzie & Corrigan, 2014). The scope of this study

was not involved in a merger of statistical testing and experiences of participants; thus, I did not decide to use the mixed-method approach. The qualitative method was the most suitable to study the security strategies in the cybersecurity infrastructure that reduced breaches because it provided in-depth exploratory information on how to mitigate cybercrime involving the healthcare organization's sensitive data.

Additional potential qualitative designs for this applied study included phenomenology, ethnography, and narrative. Researchers using phenomenology seek to comprehend more fully the richness of individuals' lived experiences (Berglund, 2015), possibly diminishing the selected depth and scope of evaluation for a study. In this study, the phenomenological design was not an appropriate alternative because I did not intend to focus on the lived experience of my participants. Ethnography focuses on protracted cultural inspection (Murthy, 2013), which was not the concentration of this study. Even though narrative inquiry incorporates interviews, the researcher asks questions that assist them in deciphering and experiencing the world of the participant rather than attempting to explain or predict the world (Wang & Geale, 2015). In this study, I sought not to qualify life, but to focus on strategies to reduce cybersecurity breaches in hospitals.

I selected a case study design for this study. The traditional case study comprises an in-depth inquiry into a particular and complex phenomenon, the case, fixed within its real-world context (Yin, 2013). I explored what security strategies the IT security managers were using to reduce cybersecurity breaches in hospitals. I chose the multiple-case design for several reasons. The multiple-case study design allows researchers to (a) delineate contextual and conflicting variables in a complex business environment, (b)

cross-reference stated opinions with secondary data sources, (c) include more than a single case in the analysis (Vannoni, 2015), and (d) generate in-depth insight into the real phenomenon under investigation (Dora et al., 2016). Therefore, multiple cases involve more than one case study to find similarities and differences.

Research Question

The primary research question underpinning this research can be stated as follows: What security strategies do hospital IT security managers use to reduce cybersecurity breaches associated with sensitive data?

Interview Questions

I used two sets of questions: (a) demographic questions and (b) interview questions. The purpose of the demographic questions was to ensure that I was talking to the right people in the three hospitals. According to Crowe et al. (2011) and Yin (2014), interview questions in a case study should enable the researcher to get information on the "what," "how," and "why" of the phenomenon under consideration. The "what" aspect was descriptive and involved information on the IT setup to combat cybersecurity risks (hardware, software, and networking). The "how" aspect was about steps and procedures used to safeguard security and how the hospital detected and responded to threats. Lastly, the "why" aspect was rational and about understanding why the hospital was investing in IT to help prevent cybersecurity breaches.

Demographic Questions

The following were the demographic questions for this study:

1. What are your roles and responsibilities within your hospital?

2. How long have you been working in this capacity in the hospital?

For Question 1, the thresholds for assuring the educational level of an individual to be interviewed included such roles as IT security problem-solver and rapid decision-maker. In terms of responsibilities, an educated individual included one who (a) analyzed IT security requirements to evaluate security risks, (b) applied safety procedures and data recovery plans, (c) responded to privacy breaches and malware threats, (d) worked as a security expert and conducted training when needed, and (e) outlined policies and guidelines.

The demographic thresholds for question two included a minimum of 5 years in an individual's current role as IT security manager; nevertheless, a person in the current role who possessed proven experience as an IT security specialist and had an analytical mind with excellent problem-solving skills sufficed.

With respect to the actual interview questions meant to capture the "what," "how," and "why" aspects of cybersecurity within the hospital, I mapped or grouped such questions into three sets of categories of interview questions, as detailed below.

What Cybersecurity Software, Hardware, and Network Environment Are Utilized?

1. Describe what software cybersecurity solutions you use to protect your hospital's IT infrastructure against phishing, malware, and hacking.
2. Describe what hardware cybersecurity solutions are implemented to tackle hardware vulnerabilities such as weakness in computer chips.
3. Describe what common networking security measures you have implemented in your network environment to combat cybersecurity threats.

How Is Cybersecurity Implemented?

1. How do you implement cybersecurity's best practices using dedicated personnel for prevention, detection, and combating comprised situations?
2. How can technology executives implement the best practices of data security with policies and procedures within the hospital IT environment?
3. How easily can intelligence about malware be distributed and acted upon within your hospital's IT infrastructure?
4. How do you implement a cybersecurity framework to investigate and remediate any cybersecurity breach in your hospital's IT environment?

Why Is Cybersecurity Important to Your Hospital?

1. Are the increased risks associated with improvements (such as electronic health records [EHR]) of IT technologies always significant to consider in your hospital? Why or why not?
2. Do you use cost-benefit analysis techniques to compare the cost and benefits of cybersecurity implementation in your hospital IT infrastructure? Why or why not?
3. Do you perform risk management for your hospital, such as choosing cybersecurity insurance? Why or why not?

Conceptual Framework

I used routine activity theory (RAT), developed by Cohen and Felson (1979a), as the conceptual framework for this study. Consistent with RAT, activities that happen daily offer random opportunities for crime and predation (Barclay, 2014). Hawdon et al.

(2017) noted that RAT specifies three features necessary for predatory breaches to occur: a motivated offender, a suitable target, and the absence of a capable guardian. RAT clarifies the criminal incident that allows three significant features that join in space and time in the process of daily activities. The three notable features are (a) a potential offender with the ability to commit a crime, (b) a suitable target or victim, and (c) the absence of guardians able to safeguard the victims. Hence, with the concurrent existence of all three aspects, a crime happens (Densham, 2015). Thus, the absence of one of the three components of RAT can reduce the likelihood of a cybersecurity breach.

Against this backdrop of information, I embraced RAT to study the security strategies in place to reduce cybersecurity breaches in the hospital organization's computing infrastructure. The key benefit of a cyber-focused theory is that it brings more accuracy and precision to studies investigating online behaviors (Choi, & Lee, 2017). I applied the concepts of the three elements of RAT to explain how cybersecurity breaches can occur in hospitals and how having security strategies in place can reduce their occurrence. I attempted to use RAT's three elements by aligning a potential offender with the ability to commit a crime to the hacker, a suitable target or victim to the hospitals' sensitive data, and the absence of a guardian able to safeguard the victims as the lack of security strategies.

Definition of Terms

The following technical and operational terms may have multiple meanings or may be unfamiliar to the readers of this study on cybersecurity and hospitals.

Information security (InfoSec): Denotes securing information or data stored and verifying that the information is not vulnerable to unauthorized access for fraudulent purposes (Bernik & Prislan, 2016).

Information technology (IT) manager: Person responsible for implementing and maintaining an organization's technology infrastructure (Yu et al., 2008).

Routine activity theory (RAT): A theory of criminology in which crime happens when three mechanisms exist in time and space: (a) an individual motivated to commit the offense, (b) a vulnerable victim who is suitable, and (c) lack of protection to prevent the crime (McNeeley, 2015).

Assumptions, Limitations, and Delimitations

In this section, I focus on the assumptions, limitations, and delimitations that underpinned my research. In their totality, the assumptions, limitations, and delimitations essentially delineate the boundaries and scope of my study but also describe the perceived weaknesses of my research.

Assumptions

Research assumptions are defined as segments of information assumed to be acceptable for a verified theory (Foss & Hallberg, 2014). Researchers make assumptions about (a) the theory under investigation, (b) the phenomenon under consideration, (c) the instrument, (d) the methodology, (e) the analysis, (f) the power to find significance, and (g) the participants in a study. Regarding assumptions about (a) the theory under investigation, I assumed that RAT is an accurate reflection of the phenomenon being studied. I assumed that RAT created a conceptual framework that was sound because it

provided the lens through which I viewed this study. For assumptions about (b) the phenomenon under consideration, my assumption was that the phenomenon was clearly defined and is measurable. As for (c) the instrument, I assumed that my role included performing the research, conducting data collection, analyzing the findings, and legitimately divulging the results. In terms of (d) the methodology, my assumption was that the multiple case study was appropriate to address the phenomenon of cybersecurity threats in hospitals. With respect to (e) the analysis, I assumed that the data were suitable to address my research question. As for (f) the power to find significance, I assumed that the analysis selected was enough to detect significant differences to the population. In terms of (g) the participants in the study, I assumed that the IT security managers answered all the interview questions honestly and that their answers were grounded on personal experiences.

Limitations

Limitations are those elements over which the researcher has no control. They include limitations regarding (a) the phenomenon being studied, (b) the theory being investigated, (c) the participant, (d) the instrument used for data collection, (e) the study methodology, (f) the data analysis, (g) the power to find significance, and (h) the results of the study (Dusick, 2015). In terms of (a) the phenomenon being studied, namely cybersecurity in hospitals, the challenge is that cybersecurity, in general, is not an absolute or a binary "0 or 100% secured" type of measure, but rather a risk measure between 0 and 100. Therefore, a limitation in this research was that it is very difficult to

define both the elements that comprise cybersecurity as well as the temporal aspects of the events that lead to such attacks and breaches.

With respect to (b) the theory being investigated, my choice for the conceptual framework to underpin my research was RAT. All three aspects of RAT can be found in the cybersecurity infrastructure. RAT can explain why cybersecurity breaches are more prevalent in hospitals' IT environment. However, RAT only presents three factors of cybercrime and neglects to address the social aspects of committing a cybercrime, such as personal education and socioeconomic status. While RAT was developed to address crime in a physical environment, cybersecurity in a hospital is in a virtual context. This limitation raises the question as to whether RAT depicts an accurate reflection of the cybersecurity approach in hospitals. Therefore, RAT provided a limited lens to explain the phenomenon under study.

Regarding (c) the participant, the limitation was that the participants would not allow me to cross-reference the information they were giving me with others in the hospital or with whatever additional documentation existed in the hospital. Cross-reference can be explained by triangulation. Triangulation is the practice of obtaining more reliable data pertaining to the research questions through adding results from various techniques, where each technique has different key sources of potential bias that are isolated to each other (Lawlor et al., 2016). Triangulation enables proof of data through cross-verification from greater than two sources. Therefore, when the participants refuse to provide other sources such as documents, they are limiting the validity and reliability of the findings of the study.

With respect to (d) the instrument used for data collection, I utilized interviews as the primary instrument to collect verbatim or textual data from the research participants. Interviews have inherent weaknesses such as subjectivity, negative reactions, and open-endedness. Subjectivity means that the interviewee speaks based on past experiences as well as possibly withholding key information. A negative reaction from the interviewer often occurs when interviewees take advantage of the opportunity to say exactly what they feel, often evading the substance of the question. Open-endedness leads to digressions during interviews. Interviews triggered digressions into mysterious specialties, wildly inventive suggestions, deviating opinions, and organizational conspiracy theories. Consequently, open-ended interview questions can generate unexpected answers to a research question.

Concerning (e) the limitations associated with the study's methodology—namely, multiple-case study, the key limitation was the sample size. In the multiple-case study of cybersecurity in the hospital, the total volume of data would be arduous to organize; moreover, data analysis and integration strategies need to be carefully considered. A significant limitation of this study was the influence of (f) the data analysis. Data analysis is unavoidably dependent on data collection. Because data collection and the data analysis process occurred concurrently, it is impossible to separate their combined impact upon this study. Data collection informed data analysis. Although data analysis programs such as Atlas.ti are helpful for sorting, organizing, conceptualizing, refining, and interpreting collected data, they are not capable of using mental acumen and conceptual processes to transform data into understandable findings.

Another of the limitations of this study was (g) the power to find significance wherein the sample size triggers constraints that impact the study. The study was limited by the comparison of the confines of the sample size of the same phenomenon. Consequently, the sample size limited the attempt to find the similarities and differences among various samples. Finally, I was not able to verify (h) the results of the study. This limitation of the verification of the results of the qualitative study was beyond my control as the researcher. Because this qualitative study was primarily open ended, the participants had more control over the content of the data. Consequently, I had no capability to verify the results objectively against the presentation of data provided by the respondents. Therefore, it was difficult to verify qualitative data such as information about strategies in place to reduce the cybersecurity breaches in hospitals.

Delimitations

Delimitations refer to the expected boundaries or restrictions that researchers use to focus on the scope of a study (Svensson & Doumas, 2013). Although cybersecurity represents a global problem, a delimitation of this research was that I only explored security strategies for the reduction of cybersecurity threats in hospitals in the eastern region of the United States. I limited this study to participants based on a census sample and include all participants who met the suitability criteria. The participants' eligibility criteria included stakeholders of the InfoSec departments of the hospitals because they had pertinent information on the hospitals' IT security. This study did not cover impact assessment and risk evaluation of cybercrime, cost-benefit analysis, and decision making on investment in the adoption of cybersecurity in hospitals. The study was limited to data

collection instruments such as interviews with hospitals' InfoSec managers and an examination of hospital IT-related documents. This study was focused on IT strategies in place to reduce cybersecurity breaches in hospitals.

Significance of the Study

Contribution to Information Technology Practice

Even though there have been some studies with a focus on cybersecurity strategies in various contexts, additional research on the specific topic related to action plans used by IT security managers to reduce cybersecurity breaches in hospitals contributes to literature and practice within the healthcare environment. Considering the lack of research on this topic, I anticipate that this study will enhance the discipline and could motivate more research on the subject.

The thematic analysis pursued in this research revealed a set of key strategies used by hospitals to increase IT security. By the nature of the interview questions, these strategies included the "what," "how," and "why" aspects of security. The purpose of the combined outcome of these three aspects was to narrow the key or most effective strategies in an easy-to-comprehend table or list. Ultimately, the significance of this list is to help the interviewees view a summary of the breadth and depth of such strategies and possibly cross-reference strategies that the other interviewees are using in their businesses to increase their security. This cross-reference may allow the case study participants to increase their accountability and possibly regulatory compliance associated with IT security.

This study is critical to IT security managers because I have recommended security strategies that are designed to improve the cybersecurity and the strength of hospitals' IT infrastructure and services. The research will be capable of giving IT security managers a robust security infrastructure for protecting a hospital's sensitive data. Safa et al. (2016) advocated compliance with organizational information security policies and procedures as a successful approach to mitigating information security breaches in organizations. The goal of this study was to highlight security strategies for IT security managers to use for the benefit of hospitals. The study's findings may benefit IT practice by augmenting written material on internal and external threats and the security strategies utilized to address them, hence increasing the comprehension

Implications for Social Change

The outcomes from this study, namely the security strategies model, once implemented correctly, may increase patients' trust and reduce threats to human life. Hackers use ransomware, malware, and phishing to steal patients' health information, which spells disaster not only for their professional life, but for their social life as well. Malicious manipulation of medical devices may affect patients' quality of life. Cybersecurity breaches undermine the trust of the patients in the InfoSec of the hospital's infrastructure. The stress of identity theft wreaks havoc for patients and customers' financial security, which lowers victims' standard of living. Consequently, InfoSec leaders in hospitals may, in effect, elevate the human impact of cybersecurity because they put in place the model cybersecurity strategies. Therefore, the security strategies from this study may prompt the security and safety of an IT-connected society. Similarly,

the implementation of the model strategies may contribute to positive social change by enhancing patients' freedom and increased protection of users' private data. Furthermore, by reducing these types of data breaches, hospitals may protect consumers against the high costs of identity theft associated with these types of data breaches. Consumers served by these hospitals may benefit from the assurance that healthcare organizations are addressing the need to protect their sensitive data from unauthorized access while providing them with excellent service through the security strategies put in place by the hospitals.

A Review of the Professional and Academic Literature

Many security strategies have been developed to reduce breaches of cybersecurity of hospitals' sensitive data. The literature review was guided by the research question: What security strategies do hospital IT security managers use to reduce cybersecurity breaches associated with sensitive data? Although the literature covers a multiplicity of such security strategies, this review focused on four significant themes that emerged repeatedly throughout the literature reviewed. These themes and the reason why they were selected were as follows: (a) the RAT framework that underpinned this research, (b) the characteristics of cybersecurity breaches in hospitals in order to identify threats to hospitals' cybersecurity, (c) current applied strategies to enhance cybersecurity in order to understand security investments, and (d) current known areas of improvement of cybersecurity in order to comprehend present implementations to countermeasure cybersecurity breaches. Although the literature presents these themes in various contexts,

this study was primarily focused on their application to security strategies for the reduction of cybersecurity breaches in hospitals.

Search Strategies and Choices

The four themes and the rationale for their selection were as follows: (a) the RAT framework that supported this research, (b) the characteristics of cybersecurity breaches in hospitals to detect threats to hospitals' cybersecurity, (c) current applied strategies to enhance cybersecurity to comprehend security ventures, and (d) current known areas of improvement of cybersecurity in order to realize the current adoption to countermeasure cybersecurity breaches.

To accumulate the information essential for this literature review, I searched through scholarly databases to compile 101 sources; these databases included Walden University Library, Google Scholar, ProQuest, SAGE, Academic Search Complete/Premier, and EBSCOhost. The search terms included *data breaches and healthcare*, *cybersecurity and hospital*, *cybercrime and health industry*, *cyberattack and hospitals*, *ransomware and hospitals*, *internal and external data breaches,* and *IT strategies for data breaches in hospitals*. My focus narrowed to literature about current themes in internal or external attacks and the strategies used to reduce them. Additionally, I selected the full-text and peer-reviewed articles published between 2014 and 2019 to limit the literature search. Table 1 contains the numbers of professional and academic sources reviewed and used in the study. There is a total of 113 sources in the literature review. Of those sources, 107, or 95%, were peer reviewed and verified through Ulrich. These sources were recent, with 101 out of 113, or 90%, of the literature review

sources having a publication date within 5 years of expected chief academic officer (CAO) approval.

Table 1

Review Literature and All References Statistics

Reference type	Total count
The total number of all references:	96
The total number of all references 5 or fewer years old	73
Percentage of all references 5 or fewer years old	76%
The total number of all peer-reviewed references	79
Percentage of all peer-viewed references	82%
The total number of all peer-reviewed references 5 or fewer years old	61
Percentage of all peer-viewed references 5 or fewer years old	63%

Data breaches remain a common occurrence, as demonstrated with recent attacks on Hollywood Presbyterian Medical Center and Unity Point Health (Yadron, 2016). Scholarly references to those attacks are minimal; however, research continued far spread. In instances in which I found sources that were more than 5 years old, I either countered or added to them with more recent work. The literature review for this study began with the conceptual framework, RAT, underpinning this doctoral study.

Routine Activity Theory

The conceptual framework for this study was RAT, developed by Cohen and Felson (1979a). The underlying concepts of RAT stipulate that for a crime to be committed, it must involve (a) a motivated offender, (b) a suitable target, and (c) the absence of a capable guardian (Hawdon et al., 2017). To better understand RAT, four attributes denoted by the acronym VIVA (value, inertia, visibility, and access) may influence whether the target is suitable and define its level of risk (Cohen & Felson,

1979a; Felson & Clarke, 1998). RAT clarifies the criminal incident that allows three significant features that join in space and time in the process of daily activities. The central issues addressed here are the three essential features of RAT: (a) a potential offender with the ability to commit a crime, (b) a suitable target or victim, and (c) the absence of guardians able to safeguard the victims. Schaefer and Mazerolle (2017) stated that at the point where all three features are present, crime is likely to occur. The absence of any one of the elements may be sufficient to prevent the occurrence of crime. These arguments suggest that when security strategies are absent, crime may occur. Reyns and Henson (2016) claimed that the number of people victimized by computer criminals has been increasing. In this context, it is worthwhile to consider RAT's application to hinder hackers' or cybercriminals' attacks on other individuals' computers without the authorization of the owners.

Evolution of Routine Activity Theory

Rational choice theory is the root of RAT, and it outlines the most cost-effective means to reach a particular goal deprived of highlighting worthiness. According to Homans (1974), although earlier propositions were based on behaviorism, the rationality proposition shows the influence of rational choice theory on his approach. He purported that people weigh and calculate alternative choices available to them (Homans, 1974). Rational choice theory predicts that humans always elevate the expected advantage of preferences when making decisions (Hewig et al. , 2011). Hence, rational choice theory postulates that humans make decisions in a rational manner, implied their behavior is modeled; therefore, predictions can be made on future activities. Proponents of rational

choice theory posit that crime is a cognitive learning behavior with the purpose of satisfying offenders' regular needs, such as status, excitement, sex, and money (Brantingham & Brantingham, 1993). The basic tenets of classical criminology formed rational choice theory's foundation. In contrast, Cohen and Felson (1979a) developed RAT from the criminological application of rational choice, and they focused on the features of crime rather than the features of the offenders. Consequently, to the detriment of psychological motivation, RAT analyzes the criminal event (Brantingham & Brantingham, 1993). Regarding RAT, RAT's milieu has a role in the happening of crime, and RAT is viewed as a characteristic of crime prevention theory.

Based on prominent studies conducted after World War II, Cohen and Felson (1979b) posited that increased crime rates resulted from structural pattern changes in people's daily activity. They hypothesized that postmodernity triggered the collision of space and time of likely offenders with criminal intention against suitable targets and without capable guardians (Cohen & Felson, 1979b). With important implications, they generated two noticeable notions: First, the makeup of criminal behavior influences the opportunity for crime; second, to prevent a potential criminal event, remove one of the three tenets of RAT (motivated offender, a suitable target, and the absence of capable guardians; Cohen & Felson, 1979b). At the macrolevel, RAT is an effort to identify criminal activities and patterns with the understanding of changes in crime rate trends (Cohen & Felson, 1979b). Although rational choice theory is grounded in the search for offenders' motives, RAT is based on criminal events and the distribution and grouping in space and time of its three components (Beauregard et al., 2007). RAT offers a context

for actual and tailored crime analysis, and it facilitates the application of real policies and practices focused on changing the essential components that make the occurrence of a crime a reality, therein preventing it (Tilley, 2014).

In their original article, "Social Change and Crime Rate Trends: A Routine Activity Approach," Cohen and Felson (1979a) elucidated a significant sociological enigma: In the 1960s, even though there were improved signs of well-being and socioeconomic situations, such as prosperity, low employment rates, and improved education, the trend showed a considerable increase in crime. They explained this seeming anomaly by shifting the focus toward changes in structural patterns of people's daily activity and how new settings triggered greater criminal opportunities, thereby resulting in increased crime rates for particular types of crime, namely property or persons (Felson & Cohen, 1980). Therefore, Cohen and Felson (1979a) shifted the focus on the situations of crimes from the offenders to the event of the crime per se.

Developed as a purposeful and straightforward explanation for changes in violent crime trends, RAT addressed changes in normal daily activity. Moreover, the changes in normal daily activity promoted an enjoyable modern life, which motivated the committing of crimes. In contrast, distinguished from criminological theories focused on the offender's motivations, RAT emphasized crime as an event that happened in a real place at a particular time. Furthermore, RAT offered a formidable tool for crime prevention and analysis because it conceptualized apart from the three elements of a crime and their supporting controllers.

Recent research findings have shown that changes in modern society had enormous significance to activities outside the home. Felson and Boba (2010) argued that RAT showed neither social pathology nor risky routines, which resulted in the increase in crime and victimization; in contrast, the normal structures of "everyday life" such as abandoning the home and going to work provided more opportunity for crime. For instance, more women's absence from home due to achieving higher education and joining the workforce left homes empty and unprotected. Other causes of leaving homes unguarded included an increase in vacation length, out-of-town travel, permanent relocation, and increased interaction with possible offenders. Thus, it could be argued that the architectural, design, and electronic hindrances or enhancements in daily life influenced the necessity to burglarize homes left unguarded (Hollis et al., 2013). Furthermore, technological advances in modern society resulted in the appearance and usage of small electronic devices such as televisions, smartphones, tablets, and laptops with higher values and lower weights, attracting theft and secure exchange for money. Finally, the flooding of cyberspace with banking and investment transactions and the sharing of personally identifiable information (PII) increased the visibility and mobility of consumable components (Shamsi et al., 2016). Consequently, the growth of available components, the multiplying of unguarded homes, and the increased probability of the collision of offenders with persons or their properties resulted in a spike in suitable targets and an increase in the absence of capable guardians to reduce crimes. Thus, a milieu of more opportunity to commit crimes directly developed from the combination of the situations mentioned above.

Cohen and Felson (1979a) examined their theory to explain the increased crime rate through scientific testing of their primary tenets. They relied on research studies that supported their hypotheses empirically (Groff, 2007). These claims included the spreading of activities outside the family and home, which could have increased the probability of a suitable emerging target, thereby diminishing the existence of capable guardians. Likewise, the suitable targets provoked predatory contacts, and lonely lives resulted from leaving the family environment, thereby increasing victimization rates (Massey et al., 1989). Moreover, they attempted to confirm that the rise in crime was triggered by changes in the fabric of Americans' daily activities. Cohen and Felson (1979a) applied Hindelang's (1976) victimization surveys to support the hypothesis that activities conducted further from home solicited higher risk than those done at home. Furthermore, they clarified the household activity ratio, which produced an estimate of the number of American households most likely vulnerable to the risk of property or personal victimization (Tseloni & Pease, 2015). American households were exposed to multiple criminal violations because myriad family members were absent from the home due to going to schools, workplaces, and entertainment events.

Three Elements of Routine Activity Theory

Cohen and Felson explained RAT with the criminal event through three essential components converging in space and time during daily activities: (a) a potential offender with the capacity to commit a crime, (b) a suitable target or victim, and (c) the absence of guardians capable of protecting targets and victims.

According to Felson and Cohen (1980), a potential offender could be anyone with the intention to commit a crime and with the ability to accomplish it. Gottfredson and Hirschi (1990) stipulated that a likely offender is most assuredly a young male without a stable job who has failed in school, has recorded traffic accidents, and has visited the emergency room. Felson and Cohen (1980) changed the term "motivated offender" to just "offender" as they refuted the relevance of disposition or mental stimulation to commit a crime, emphasizing instead the existence of the physical factors enabling a person to commit a crime (Felson & Boba, 2010). Consequently, Felson (Eck & Weisburd, 1995) shifted the focus to the crime instead of the offender. Although Felson (Eck & Weisburd, 1995) found it necessary to include other features of crime for comprehension and prevention of the act (Felson & Clarke, 1998), he sustained his concept of the offender (Felson & Boba, 2010). Subsequently, the understanding of the purposes and capacities of the assailant in relation to inherent characteristics of the potential targets of crime resulted in the definition of the target as "suitable."

An offender may threaten a suitable target, which may be either a person or a property. Although the victim, who may be absent from the crime scene, fits the description, Felson and Clarke (1998) preferred the term "target" because it highlights the fact that the purpose of the majority of crimes is obtaining goods. Described from the perspective of the offender, the acronym VIVA (value, inertia, visibility, and access) captures the factors that influence the probability that a target will be suitable (Felson & Clarke, 1998). From the perspective of the offender, each element of VIVA may be explained as follows: (a) “value” could either be real or symbolic; (b) “inertia” refers to

size, weight, and shape, or the physical features of the person or property that act as obstacles or obstructions to the offender considering the target suitable; (c) “visibility” or exposure of targets denotes the element that identifies the person or the good for the incident; and (d) “access” refers to the design of the site and the position of the object that amplify the risk of attack or make it easier to do (Felson & Clarke, 1998).

The understanding of a suitable target in RAT is itself composed of several mechanisms, captured in the acronym VIVA. Researchers have explained the model features that affect the suitability of a target. They have classified these features as VIVA: value, inertia, visibility, and access (Felson & Clarke, 1998). Hence, value denotes the monetary value of the target, inertia indicates the weight of the target, visibility involves how visible the target is, and access pertains to its availability (Vakhitova et al., 2015). For a motivated offender such as a hacker working against the cybersecurity of a hospital’s IT environment, one valuable suitable target is PHI; the inertia of the target is the light weight of digital information, the target is visible, and the target is accessible because of lack of guardianship and security strategies. Likewise, prior researchers have claimed that target suitability is determined by VIVA (Leukfeldt & Yar, 2016; J. Wang et al., 2015). Furthermore, Lee et al. (2018) argued that information about these features, VIVA, might be readily available to the motivated offender in cyberspace. The benefits of cyber resources regarding information for motivated offenders' scrutiny of the target's value, inertia, visibility, and access might prove detrimental to the suitable target, PHI.

To expand on the VIVA concept, Cohen and Felson (1979a) modified their

superficial description in their initial work. Moreover, they applied the VIVA concept to material or personal targets. Without focusing on the motives that trigged the offender to choose one target versus another, the authors paid attention initially to the relationship of the target to space and time, consistent with their ecological perspective. After Cohen and Felson (1979a) developed RAT, complemented by other theories such as rational choice theory, they created enough distinction between RAT and theories of criminality. Subsequently, they supported the theory with empirical research, and later they formulated new concepts—Clarke's "hot products" (1999), for example, which focused on the most compelling items to thieves. Furthermore, Clarke and Webb (1999) used the acronym CRAVED, describing frequently stolen products that are concealable, removable, available, valuable, enjoyable, and disposable.

According to Cohen and Felson (1979a), in theory, the third and final element is the absence of a capable guardian, a person able to stop or hinder a crime. Moreover, with the ability to prevent a crime, the capable guardian whose presence no crime is committed and whose absence created the likelihood for the occurrence of a crime (Felson, 1995). Although the idea of a guardian should neither be confused nor restricted with security guards or police officers, the concept includes anyone moving through a location or guarding property or persons. Such capable guardians are often absent at a crime scene (Felson & Boba, 2010). The classic Kansas City Preventive Patrol Experiment, tested the effectiveness of random patrols, indicated that an increase from routine patrol levels in a particular region produced a minimal effect on criminal activity in the region (Kelling et al., 1974). Furthermore, examples of other capable guardians,

considered significant personnel in crime prevention, include any person such as a brother, a friend, passer-by, or house-occupant. Consequently, any person, while doing his or her everyday routines, may protect any of the lists of objects: himself, herself, others, his property, her property, or others' property.

Since its first formulation, the notion of the capable guardian (present or absent) was exposed to updates. Besides other researchers, Felson debated and reformulated its definition. Hollis-Peel et al. (2011), in a literature review of the guardian figure in RAT, defined guardianship as the symbolic or physical presence of an individual (or group of individuals) whose presence limits a potential criminal event. Such definition included elements that the authors held as inadequately specified in both the original article by Cohen and Felson (1979a) and subsequent works. Hollis-Peel et al. (2011) cited the example, closed-circuit television (CCTV), operated by people whose presence at the physical crime scene is non-existent. Felson (1995, p. 54), in an attempt to connect RAT to Hirschi's social control theory (1969), redefined the character of the guardian when he differentiated the "place manager" from "intimate handler." While the first character, guardian, stipulated those persons such as doormen, bus drivers, and valets having a supervisory role in specific places; the second character, however, would be a parent or friend who attempted, through the resistance of the potential offender's conduct, to deter actions that break the rules. Therefore, in formulating the concept of the guardian, Felson adopted the four elements (attachment, commitment, involvement, and belief) of Hirschi's theory (1969) and developed one idea, "handle." Consequently, in stipulating the notion that someone is capable of dissuading an offender through his or her presence,

or, someone discouraging a potential offender due to his ties with him, Felson's upheld the notion of social control and emphasized the idea that control remains a critical element in crime rate trends (Cohen & Felson, 1979b).

Together with the knowledge of Cohen and Felson's three initial elements (offender, target, and guardian) and their later developed intimate handler, Eck (1994) formulated the crime triangle, distinguishing the elements needed for a crime to happen from controllers with the potential to prevent crime. Located in the inner circle are offender, target, and place, while in the outer triangle are controllers that supervise them. By controlling each of these three elements, the controllers could reduce the probability of a crime occurrence. Consequently, handlers are persons whom the offender relates to emotionally, whether through friendship, family, respect, religion, or others. Moreover, the handlers intend to restrain the potential offender from problems. Likewise, place managers are owners of the place or their representatives, such as store employees, servers, doorkeepers, or others who endeavor to avoid problems in the place. Lastly, guardians, who are security guards, police, and owners, aspire to defend the target and guard vested properties.

Concerning these concepts, Felson (1995) rationalized the probability that the place manager, the handler, or the guardian who carried out their assigned tasks should be explored in contingent to his or her level of responsibility. He instituted four distinctive levels: (a) personal referred to friends, family, or owner; (b) assigned denoted employees given responsibilities for taking care of a place; (c) diffuse referred to employees assigned generic responsibilities; and (d) general denoted the responsibility of any

individual. He designed a four by three metrics with 12 cells where the rows are levels of responsibility and are crime elements and their corresponding controllers in the columns. Hence, a given component provides the ability to analyze the probability of a controller's success based on the level of responsibility. A guardian, who is an owner, watching his or her luggage, would have the lowest risk of it being stolen. In a case where a security guard was watching it, the risk would be lower; however, if the watcher were an employee with separate duties, the risk would be greater; yet, if a watcher had no relationship with the luggage owner, then the risk would increase.

Analyzed the rationale for ineffective or mistaken actions of controllers, Sampson et al. (2010) developed the notion of "super controllers," which are organizations, institutions, and people that provide controllers with incentives to either facilitate or prevent crime. Moreover, the super controllers, lacking the direct influence of the elements, may indirectly incentivize crime prevention. Therefore, in the extension of the crime triangle, they added a third group of factors surrounding three categories (formal, diffuse, and personal) and ten types (contractual, courts, financial, family, group, market, media, organizational, political, and regulatory).

During the past decades, RAT theory underwent many developments and applications. Given its robust and pragmatic propensity, it primarily focused on preventing crime by reducing opportunities. Likewise, the underpinning perspective of rational choice and the notion of the controller presented by RAT emerged the theory's circumstantial crime prevention. Moreover, it focused on changing the makeup of specific crime opportunities through various techniques, therein increasing risk, mounting

effort, removing excuses, and reducing benefits. Furthermore, other researchers analyzed places whereby the crime happened, to elucidate the spreading of crime in space relating to RAT. Hence, looking for differences among cities or countries or demonstrating focuses on certain areas. Sherman et al. (1989) performed a study in the city of Minneapolis wherein they discovered that 50% of emergency calls to law enforcement came from 3% of urban areas, while robberies were limited to 3.6% of the city. Consequently, this theory predicted victims' victimization, characteristics, and behaviors.

Researchers analyzed the relationship and application between RAT and cybersecurity to better understand the rationales behind cyberspace behaviors. There is evidence that researchers used RAT as the lens for viewing information technology security research in analyzing the differences between vulnerabilities in a milieu and adopted protections and safeguards established within an environment (Khey & Sainato, 2013). Moreover, researchers applied RAT as a conceptual framework that increased the understanding of cybersecurity threats in hospitals. Against this backdrop, researchers posited that RAT might be attracted to a potential offender of crimes due to their association inherently appealing to that individual (Holt et al., 2018). Therefore, a deeper understanding of the offender's motivation might be the central driving force that propels their actions.

When researchers analyzed RAT, they often emphasized the portrayal of the three elements of RAT: (a) a motivated offender, (b) a suitable target, and (c) the absence of guardians. Cohen and Felson (1979a) stipulated that the likelihood of crime happening increases with the convergence of the three components in time and space. Choi et al.

(2016) agreed with the three mechanisms of RAT, a motivated offender, a suitable target, and the absence of a capable. Other researchers emphasized that the three elements increase the probability of cyberbullying victimization (Elmaghraby & Losavio, 2014). The joining of these elements increases the likelihood of crime; the non-existence of a component lessens it (Elmaghraby & Losavio, 2014). RAT is capable of: (a) suggesting potential vulnerabilities, (b) recommending improved IT security, and (c) ensuring data security.

Routine Activities Influence Cyber Victimization

Routine activities of hospitals happen in the cyberspace environment of the Internet and health IT network where the elements of the RAT converge. Accordingly, Cohen and Felson (1979b) elucidated that the occurrence of crime resulted from merging a motivated offender, a suitable target, and the absence of capable guardianship. The application of Cohen and Felson's explanation of digital time and space appropriately identified the meeting place as the Internet. For this purpose, the Internet has changed opportunities for cybercrime and cybersecurity threats used by hackers and other cybercriminals (Pyrooz et al., 2015). Therefore, the advancement of IT and the popularity of the Internet are considered routine activities milieu of the hospitals' organizations since the 1990s. Before the exponential growth of the usage of the Internet, motivated offenders and suitable targets (victims) had to share the same physical environment somehow; however, Zaharia et al. (2010) argued that online environment or cyberspace provides an offender and a victim the opportunity to converge without co-existing in the same physical space. Moreover, one of the primary challenges hospital professionals

confront is the transition of their behaviors performed in controlled environments to routine clinical practices in national hospitals (Demarzo et al., 2015). Routine activities of hospital stakeholders, such as nurses, doctors, administrators, administrative assistants, radiologists, lab technicians, and other employees, include accessing the healthcare network with their computers. Furthermore, based on RAT, Agustina (2015) demonstrated the significance of the behavior of victims in cyberspace perspective in showing cybercriminal events and developing strategies to reduce cybersecurity breaches. Therefore, there is a correlation between the hospital's personnel, especially within the virtual contexts, and their disinhibited behaviors in their routine activities.

Supportive Theories. Earlier ecological theories, such as Shaw and McKay's (Shaw et al., 1929) social disorganization theory and Hirschi's social control theory (Hirschi, 1969), recognized some elements of the criminal event in space and time. Cohen and Felson (1979b) identified the socio-environmental feature of the crime event, and through the emphasis on routine activities, they offered a power-filled model explaining the "ecological" nature of crime and showed how elements, seemly separated from the illegal activity, affected the shape, and decided it. The offenders may use many technological advances intended for legitimate purposes, such as electronic devices, highways, railways, airplanes, smartphones, and computers, for their illegal activities (Choi & Lee, 2017). Consequently, the makeup of lawful routine activities determines how crime is completed in society and where it happens.

Amos Hawley's human ecology theory of community structure is the focal root of routine activities theory. Authors such as Guerry or Quetelet studied spatial variations in

crime rates; the research, however, had hardly explored the temporal interdependence of crime with human activities and place (Andresen, 2011). In their seminal research, Cohen and Felson (1979a) zeroed in on patterns of human activity as purported by the work of Hawley, who posited that community is more than a mere territorial unit but also a symbiotic society of human activities that happen in space and time. Consequently, to understand society, the three elements (rhythm, tempo, and timing), in which the organization of time is divided must be studied.

Even though its underpinning is in human ecology, RAT allows many connecting points with other criminological theories. These criminological theories, such as criminal justice theories, deterrence, and rational choice theory, or psychological theories of crime, influenced RAT (Eck & Weisburd, 2015). Moreover, approaches of intervention in the 1970s that postulated criminals as individuals needing psychological or medical treatment for their behaviors affected RAT (Taylor, & Gunn, 1999). In contrast, approaches such as rational choice operate from a realistic viewpoint of intervention in circumstantial factors and criminal milieu. Cornish and Clarke's (2008) work possessed such a view of intervention, which intersects with the initial vantage point of Felson's approach (rational decision). Furthermore, this approach focuses on crime prevention and clarification of both the criminal and the environment of the event (Eck & Weisburd, 2015). Rational choice suggests an offender's conduct explore to acquire a benefit. Likewise, rational choice posits that the offender decides on the foundation of a determination made after rationalizing their opportunities to perpetrate a crime successfully, the risk of being apprehended and the profits hoped to achieve (Paternoster

et al., 2015). Two decisions (involvement and event) formed the process of such cost-benefit analysis (Cornish & Clarke, 2008). Consequently, the first denotes a proclivity to commit crimes whereby the person evaluates the various choices on the table to acquire his or her objectives and eventually chooses to commence offending and proceed or refrain (Mustaine & Tewksbury, 2000). The second, specifically, refers to crime influenced by circumstantial factors. Nevertheless, a rational decision means that the criminal made a passionate calculation of each choice along with its outcome; likewise, the criminal, in his or her viewpoint and outlook, is susceptible to making mistakes. Therefore, unknown to the offenders, the criminal's decision is limited by numerous variables that affect their behavior.

Initially, Cohen and Felson's (1979a) approach remained consistent with the notion of a rational criminal taking advantage of opportunities. Likewise, an opportunity presents a pertinent role in the emphasis on routine activities along with the viewpoint of rational choice. Limited to the victim's role, Hindelang's lifestyle theory (1976) was one of the first instances of the opportunity paradigm. Moreover, Hindelang's lifestyle theory's central notion is that certain lifestyles prefer victimization since they offer it more opportunities. Considered one of the great milestones of opportunity theories, the work of Mayhew et al. in London (Mayhew et al., 1976) contributed considerably. Although it existed with the approach of Cohen and Felson (1979a), the British theory was perceived as independent of the development of RAT because of the non-existence of references from research in London (Tilley, 2014). Consequently, RAT postulates that crime rates may rise or fall independent of any change in the criminals' count. Moreover,

the rise in suitable targets' availability or the decreasing effect of guardians or society's routine activities changes may increase the probability these elements meet in space and time; therefore, increased opportunities for crime. Predominantly, RAT posited opportunities as unevenly distributed in society, and they are unending. In contrast, criminals may find attractive a limited number of available targets (Tillyer & Eck, 2009).

Ultimately, crime pattern theory emphasizes the spatial connectors among targets and crime and predicts the movement of offenders whose routine activities happen in times and places wherein there is a greater likelihood of committing illegal actions. Incidentally, offenders perpetrate their criminal acts in the proximity of where they hang out, such as school, shopping, home, work, and entertainment, as well as nearing the interconnected routes. Activities are undertaken in the past, and conditions that placed their future events determined the offenders' awareness of the surrounding spaces. Therefore, understanding the spatiotemporal distribution patterns of crime demands knowing the criminals' living patterns and activities.

Researchers developed RAT during the rise of victimization taking precedence. The emphasis shifted for both the victim and the offender. Several theories that support RAT include human ecology theory and lifestyle exposure theory (Vakhitova et al., 2015). These theories have similarities with RAT but tend to defer to causes of crime. The core concepts of human ecology theory and lifestyle exposure theory are that individuals' daily activities promote victimization, either in real life or digital. In 1950, Hawley (1950) created the human ecology theory, which taught that the interaction of an individual with his or her milieu would propel him or her to commit a crime. Likewise,

lifestyle exposure theory stimulates individuals' actions based on their interaction with their surroundings (Schaefer & Mazerolle, 2017). Even though RAT concentrated primarily on computer victimization, it stipulated that an individual's daily activities would propel him or her into criminal activities. Therefore, all three theories, human ecology, lifestyle exposure theory, and RAT, come to similar conclusions.

Contrasting Theories. While the same logic underlies human ecology theory and lifestyle exposure theory address similar concerns as RAT, they differ in several ways. Human ecology theory focuses exclusively on individuals' physical acts against one another (Hawley, 1950). Hence, human ecology theorists concentrate on only the physical crimes perpetrators commit against their victims. This behavior leads to the lifestyle exposure theory, followed later in response to technological growth. The primary aim of lifestyle exposure theory deals with computer victimization (Bunch et al., 2015). As noted earlier, lifestyle exposure theory claims certain lifestyles culminate in the happening of computer victimization. Lifestyle exposure theorists correlated leisure time and its effect on computer victimization. Although lifestyle exposure theory and RAT are similar in how they view victimization as the convergence of a motivated offender, an attractive target or victim, and the absence of a capable guardian, they differ in viewing the behaviors that put at risk the people's safety (Pratt & Turanovic, 2016).

The routine activities and contagion theories of situational crime are comparable and distinctive. The deficiencies of each theory make them distinguished. Although the RAT emphasizes the confluence of crime, contagion theory focuses on the transmission of crime. (Degarmo, 2011). Confluence denotes the offender and victim converged in a

suitable crime location at a particular time. In contrast, contagion scrutinized the method a singular and aggressive emotion spread from individual to individual irrespective of location or time. Consequently, RAT touches on one crime or crime density in a location instead of examining a series of inter-correlated crimes. RAT scrutinizes much crime happening in a "hot-spot" area (Weisburd et al., 2006); however, contagion would examine how law enforcement aggression in hot-spot areas escalates crime via payback violence or genuine contagion wherein either law enforcement agents are directly victimized, or civilians are later victimized.

Critique of the Theory

The primary arguments against RAT include its efficacy, moral and political legitimacy, and propensity to accuse the victim. Proposed primarily by a group of authors with traditional criminology, they critique RAT with theories pertaining to criminality and their preventive models (Clarke & Felson, 1993; Cohen & Felson, 1979a; Felson, 1995). Concerning the RAT's efficacy, the primary critique is that the theory's tactical actions have no natural effect in curving crime because the result is the displacement of the elements of RAT such as place, target, method, time, or form of the crime. Moreover, some authors criticized the opportunity and rationality components of the theory (Hirschi & Gottfredson, 2008). Critics argued that even though the theory's foundational notion of the rational decision applies to minor offenses with a minimal emotional component, it is irrelevant to violent crime (Akers, 1998). As it relates to opportunity, critics claimed that RAT and other crime theories confused the issue of whether places can change their ability to cause crime; however, they argued the crime

would happen anyway since the opportunity presented itself.

Lastly, moral legitimacy is the area critics use to attack RAT severely. Argued that the focus on routine activities showed neglect of the offender, and the detractors advocated RAT's disregard of the etiology of the problem (Massey et al., 1989). They accepted that RAT's basis highlighted the existence of a "motivated offender" but undefined its meaning. In contrast, the critics claimed Cohen and Felson still have unanswered questions such as "Who are motivated offenders," What are their features? And "Why are some individuals more motivated than others to commit crimes?" (Akers, 1997). Regarding the issue of motivation, other authors analytically maintained that motivation is chained to opportunity because both elements described the criminal event (Osgood et al., 1996). The critics stipulated that RAT effortlessly adapted to social and economic policies to the detriment of groups of people (Reyns & Scherer, 2019). Critics advocated that RAT completely embraced "zero tolerance" law enforcement policies associated with subjugating minor crimes (Garland, 1999). Therefore, the foremost arguments used to reproach of RAT critique its efficiency, political and moral legitimacy, and tendency to accuse the victim.

Since 1979, RAT has significantly impacted criminology, and attracted essential empirical support. Together with rational choice and crime pattern techniques, it continued a close relationship with crime analysis and prevention. Moreover, with a substantial degree of effectiveness, RAT is applied to strategies such as problem-oriented policing, problem analysis, and situational prevention. Most critics postulated significant criticisms of its ethical and methodological foundations, and stipulated its insufficiencies

and risks; however, they are incapable of denying its competence to articulate and elucidate the necessity to explore crime by preventing it. Therefore, when the critics pay attention to RAT's explanation of the increase in crime trends, they observe as daily life progresses in various places.

Through the years, RAT has had a significant impact on criminology and has received important empirical support. It maintains a close relationship with crime analysis and prevention along with rational choice and crime pattern approaches. It has been applied to strategies such as situational prevention or problem-oriented policing and problem analysis with a significant degree of effectiveness. Although there have been important criticisms of its ethical and methodological underpinnings, the majority of critics articulate its limitations and risks but are unable to deny its capacity to express and explain the need to look at crime, in order to prevent it, by paying attention to the daily life unfolds in different places.

Usage of RAT. Using logistic regression, Navarro and Jasinski (2012) found that the RAT is a viable explanation for cyberbullying risk among teenagers. Cyberbullying is when an individual or a group resort to using information and communication technologies such as email, smartphone, instant messaging, or intimidating and threatening websites to bully a person(s) through repeated, hostile, and deliberate behavior (Bauman & Yoon, 2014). Cyberbullying denotes posting harmful text or images using the Internet or other digital communication devices. Navarro and Jasinski (2012) used data from a national sample of 935 teenagers, and they examined the ability of routine activities theory to predict cyberbullying

Consequently, RAT is significantly used to study other categories of crime, such as sexual crimes (Tewksbury & Mustaine, 2001), robbery (Tseloni et al., 2004), and currently cybercrime (Miró, 2014). Moreover, Miró (2014) described the intrinsic and extrinsic features of cyberspace and considered the question of whether it provides a different milieu of criminal opportunity

Through the adjustment of Felson and Cohen's RAT, RAT is credible to make a synopsis of how to reduce cybersecurity breaches in hospitals. Academics used RAT, an established and widely mobilized theory, to scrutinize different forms of criminal conduct (Leukfeldt & Yar, 2016). The focus of RAT is on crime at the occasion level and understanding the significant ideal conditions for an offense to happen at a particular time and space. According to Johnson and Groff (2014), RAT conditions highlight the network between elements that produce crime prospects and, at last, crime incidences. The application of the RAT to cyberspace is very relevant during the 2010s.

The use of RAT to explain the happenings of global criminal acts benefits our understanding; however, the drawbacks of RAT provide challenges. One such example is the issue of the provision of testable propositions on capable offenders. Bunch et al. (2015) claimed that the RAT is unusable for establishing an extensive investigation of computer victimization. Of equal importance, Felson and Cohen (1980) did not explain what motivated offenders in their perpetrations. They conceded that motivation was persistent. They avoided describing how an individual's social status affected his or her actions. Some notable examples of a social feature such as poverty may influence an individual's actions. A conflicting viewpoint is that the RAT covers a given section of

crime; but neglects to address some types of offenses.

Technology-enabled crime theories such as RAT and other discussed theories, human ecology theory, and lifestyle exposure theory were helpful for the investigator to explain the data research proposed in the current study. According to Stratton et al. (2017), the concept of 'digital society' focuses on the rise of new techno-social techniques of both justice and crime and the persistent bearing of cultural, social, and critical theories of society in comprehending and reacting to crime in a technology-enabled time. While the existence of investigation supporting the use of RAT, human ecology theory, lifestyle exposure theory, and other technology-enabled crime theories to cybercrime, other research considering RAT and cybercrime perpetrations is insufficient. I analyzed these elements to further the comprehension and study of strategies for reducing of cybersecurity breaches in hospitals.

RAT applies to this study because it provides an in-depth understanding of the rationale for individuals to involve in cybercrime in hospitals. Miró (2014) outlined the correlation between increases in cybercrime and other intelligence-gathering philosophies such as RAT. The use of RAT as the conceptual framework for this study is appropriate for examining and describing cyberattacks in hospitals. RAT was applied experimentally to different cyberattacks and noted some of the procedural concerns demanded. The knowledge and understanding of cybercriminals' new techniques resulted from enabled crime theory due to technological applications. Furthermore, scholars of IT used crime theory to assist with the awareness of new types of aberrances and social mishandling of several crimes through the thought of change.

Felson and Cohen (1980) used RAT by Felson to elucidate the episode of various crimes worldwide. Although not undoubtedly applicable to all crimes, the theory has exposed the process of what is happening in many criminal endeavors. Typically, most of the analyses performed today demonstrate support for the RAT theory (Leukfeldt & Yar, 2016; Reyns & Henson, 2016). The theory's emphasis was on computer victimization, which is increasing and encompasses people of all ages. The theory cogitated and discharged the factors promoting criminal incidence; concluding that an amalgamation of factors leads to criminal incidences. This conclusion has aided in imminent research in addressing security issues.

Cybersecurity Breaches in Hospitals

Hospitals' stakeholders face severe challenges coupled with the increasing threats in shielding confidential Protected Health Information (PHI) from cybersecurity breaches. Perakslis and Stanley (2016) argued that since 2012, almost all healthcare organizations have had at least one data breach. These cybersecurity breaches involve the degradation of the goals of information security, such as confidentiality, integrity, and availability. In addition, Williams and Woodward (2015) explained how cyber attackers who gained unauthorized access to sensitive hospital information proceed to read the information to (a) obtain confidential data and sell it; (b) insert false data leading to a loss in data integrity, and (c) delete the information, making it unavailable. The triad of information security (confidentiality, integrity, and availability) are at the risk of cybersecurity breaches. Mansfield-Devine (2016) claimed a sizeable percentage of organizations affected, at some time, with cyber-criminals seemingly focusing their

attention on the most vulnerable, such as hospitals. Furthermore, the weakness of healthcare to cyberattacks exposed a mixture of factors, particularly fragmented governance, cultural behaviors, and limited resources (Martin et al., 2017). Therefore, hospitals are complicated, dispersed, and deficient in resources; however, vulnerable health information systems possess tremendous quantities of valuable and sensitive data.

Cybersecurity Characteristics and Prominence

Cybersecurity breaches in hospitals are gaining prominence. McGuire (2015) demonstrated the progressive growth of threats when he stipulated that formerly not a month would pass without some new data breach reported, and then not a week would pass by; however, now, the reports of new attack vectors are daily events. McGuire (2015) further pointed out that regularly some new cyberespionage groups, some different kinds of cyberattacks happening against the critical network and private data of multiple organizations such as the healthcare sector. Benzel (2015) agreed that cyberspace is under a relentless assault of cyberattacks, and it appears that every day publicized, yet another significant data breach. The occurrence of data breaches increased with exceptional frequency. Because many hospital IT infrastructures contain vulnerabilities, hackers can take advantage of relatively simple activities to gain entry to a wealth of sensitive information, such as social security numbers (SSN), credit card information, and valuable health records (Astani & Ready, 2016). Hence, health records provide more valuable information because they include multiple personally identifiable information (PII), such as patients' demographics, SSN, credit card information, and PHI. Romanosky (2016) showed that insurance and finance (such as insurance carriers, credit

intermediaries), healthcare (ambulatory care, hospitals), and government entities (courthouses, police, and administrative offices) suffered the highest number of reported breaches of all businesses in their dataset. Furthermore, Romanosky (2016) stated that the healthcare and financial services sectors suffered the most significant percentage of breaches from their sample. An integral part of the increase in the eminence of cybersecurity breaches is the implementation of electronic health records (EHR) and the negative openings of more data breaches.

Adopting electronic health records (EHR) in hospitals provides several benefits, but the primary drawback is making more patients' health information (PHI) available to hackers. Specifically, an electronic health record (EHR) is documentation of a patient's medical particulars, including medical history, physical examination, investigations, and treatment, in computer format (Ozair et al., 2015). Unlike patients' paper records, EHR computerized patient records, which trigger the compulsion to protect the data from unauthorized access. Likewise, the researchers Shenoy and Appel (2017) acknowledged that many EHRs are web-based and exposed to cybersecurity breaches from outside the health information system. Shenoy and Appel (2017) further elucidated that such breaches might involve a doctor or nurse losing a laptop or flash drive holding PHI on tens of thousands of patients or a coordinated attack by international hackers that could breach the security of millions of patients' sensitive data. Security breaches in hospitals might stem from either negligent or malicious healthcare professionals. In contrast, Shenoy and Appel (2017) advocated that electronic health records (EHR) can improve

patient care by making health information more broadly available. However, great diligence is required to protect sensitive data from malicious hackers and cybercriminals.

Types of Cybersecurity Breaches Trending

The different types of cybersecurity breaches in the hospital include email phishing, ransomware, exposed Bring Your Own Device (BYOD) and wireless, and vulnerabilities of medical devices. Sebescen and Vitak (2017) identified four threat categories: (a) phishing, (b) passwords, (c) BOYD, and (d) company-supplied laptops. Hence, the security risks of email phishing, compromised password, vulnerable BOYD, and stolen hospital laptops are trending. Safa et al. (2015) pointed out that hackers use various techniques to alter integrity, confidentiality, and the availability of information to align with their benefits, while users deliberately or through negligence are a great risk for information security. Cybercriminals use various methods against healthcare organizations, such as denial of service (DOS) attacks, which purpose disrupt and disable IT infrastructure by flooding them with extreme volumes of network traffic (Gordon et al., 2017). Cybercriminals employ different methods to penetrate the triad of information security of the healthcare system. Safa et al. (2015) elaborated that end users are exposing their login credentials, acquiring any apps from the Internet, stashing passwords in obvious places, and utilizing social security numbers as a password or username are some of their careless and insecure behaviors. The reasons for security breaches include users' ignorance, resistance, mischievousness, negligence, apathy, and lack of awareness (Safa et al., 2015). With such negative behaviors, end-users are considered the weakest link of hospitals' cybersecurity. Besides, Coventry and Branley (2018) agreed that healthcare is

a prime target for cybersecurity breaches for two basic reasons: a weak defense and a rich source of valuable data. The more vulnerable devices become medical devices with the addition of components to the hospitals' network,

The connection of implanted medical devices to the hospital information infrastructure might improve patient care and provide convenience for both the health providers and the patients. For instance, Coventry and Branley (2018) explained that cybersecurity breaches include stealing health information and ransomware attacks on hospitals; moreover, an emerging breach is an assault on implanted medical devices. The attacks on embedded medical devices could be life-threatening. Furthermore, Wu and Eagles (2016) pointed out that medical devices with wireless applications are exposed to cyberattacks. Wu and Eagles (2016) further stipulated how increasing cybersecurity threats redefined safety risk management in manufacturing. Consequently, the makers programmed wireless medical devices to reduce the risk of cybersecurity threats. Burns et al. (2016) suggested that fast integrated technology allows multiple ways of attaching to medical devices. The likelihood of cybercriminals finding medical devices increases because access to medical devices is easy (Coventry & Branley, 2018). Rios (2015) argued that together with medical devices becoming progressively wireless and networked is the detailed monitoring of medical devices in cybersecurity. Introducing wireless medical devices to the hospitals' information technology demands excellent oversight. Furthermore, Pycroft et al. (2016) claimed that brain-jacking, formerly thought to be science fiction, is a potential for cybersecurity breaches. Brain-jacking denoted the exercise of unauthorized control of another's electronic brain implant (Pugh et al.,

2018). Brain-jacking involves illegally controlling of implants such as pacemakers, insulin pumps, and defibrillators. The proliferation of cybersecurity breaches of medical devices had some form of impact on the hospitals' IT environment.

Impacts of Cybersecurity Breaches

Cybersecurity breaches might disturb the activities of patient care that must use the health information technology and may divert finances from patient care to mitigate a cybersecurity breach. According to Manworren et al. (2016), monitoring cybersecurity enables organizations to identify and tackle weaknesses; moreover, it helps them avoid the shame and cost of reducing cybersecurity breaches. Embarrassment and financial loss are among the negative impacts of cybersecurity breaches. Furthermore, Gordon et al. (2017) pointed out that hospitals are confronted with poor choices concerning ransomware: either pay the cybercriminal, most times namelessly in online cryptocurrencies such as Bitcoin, or trust recent backups, sometimes without the most current medical information. They further stated that even a hospital with daily IT infrastructure backups could miss critical data if required to restore from a recent backup. Hospitals' C-executives face complex decision-making when they suffer a ransomware attack, such as either paying the attacker or restoring from backup. Such cyber-attacks can cause clinical processes to become unusable with a negative impact on essential hospital functions, such as pauses in operative procedures, bed management, and lab-result reporting (Gordon et al., 2017). Even with the adoption of high-tech health information technology (HIT) systems, cybersecurity breaches continue to impact many hospitals and compromise millions of patients' data. Furthermore, Kruse et al. (2017)

claimed that there are rising anxieties that cybersecurity within healthcare is not enough, and this resulted in a deficiency of medical information confidentiality. Therefore, cybersecurity within hospitals is not measuring up to the requirements of protecting the patients' and employees' private data because the condition of information security is lacking. Protection against the effects of cyberattacks may be a portion of the liabilities insured against; likewise, hospitals are insured against claims of criminal carelessness (Martin et al., 2017). In summary, cybersecurity breaches can cause not only the disruption of the workflow of hospitals' processes but also a monetary loss to the hospitals.

The trend of data breaches influenced different insurance, such as the loss caused by cyberattacks. The significance of the cybersecurity breach resides in its far-reaching results, legislating through the U.S. Congress, and heightening consumer and industry awareness of cybersecurity (Pigni et al., 2018). Cybersecurity breach affects multiple facets of our society, from legislation to end-user security education, training, and awareness (SETA). Klonoff (2015) observed simulated cyber-attacks remotely controlled medical devices to change operations or send lethal drug doses. Simulations showing the potential cyberattacks on medical devices are only the beginning of the novel cybersecurity threat, but the reality of the actual attack occurring is frightening. Khera (2017) stipulated that starting in 2011, the cybersecurity community noticed a steady spurt of focus by both players (cyberattackers and security researchers) to learn techniques to manipulate vulnerabilities to have desired control over hospital's diagnostic machines, personal devices, and other medical appliances. Both the

cybersecurity researchers and the cybercriminals are searching for ways to control medical devices for obviously different reasons. The Department of Homeland Security (DHS) is collaborating with manufacturers to pinpoint and patch software programming bugs and other weaknesses that hackers can use to attack hospital equipment or reveal confidential data (Klonoff, 2015). The Health Insurance Portability and Accountability Act (HIPPA) legislation delegated stringent controls on the transfer of personally identifiable health data between two entities, provisions for the release of protected information, and felonious penalties for violation (Clayton, 2001). The enforcement of the HIPPA protects the privacy of every patient against digital breaches of medical devices. The government entity, DHS, is exerting its influence to work with manufacturers of medical devices to reduce the risk of cybersecurity breaches on medical equipment.

Current Applied Strategies to Enhance Cybersecurity

Having a clear understanding of cybersecurity in a hospital context explained the strategies in place to reduce cybersecurity data breaches. To better understand, the National Initiative for Cybersecurity Careers and Studies (NICCS) noted in its glossary the definition of cybersecurity as the capability or ability, process or activity, or state by which communications and information systems and the information contained within are defended against damage and are protected from exploitation, or unauthorized use or modification (Evans et al., 2016). Hospitals' cybersecurity involves strategies adopted to secure the patients' sensitive data and privacy and other hospitals' stakeholders, such as employees, vendors, and employers' confidential information. Martin et al. (2017) argued

that cybersecurity is more than protecting data; it is essential for maintaining patient privacy, safety, and confidentiality. Integrating cybersecurity strategies in a hospital demands the cultivation of a culture that permeates the entire hospital environment. Coventry and Branley (2018) agreed that cybersecurity should be a central component of patient care culture as more secure, substantive approaches must replace insecure and convenient processes. Consequently, cybersecurity means more than securing the hospitals' information technology, such as complying with policies and regulations and integrating security into the culture. Furthermore, Jalali and Kaiser (2018) stipulated that to heighten cybersecurity potentials at hospitals, the primary emphasis of chief information security officers (CISO) and chief information officers (CIO), should be on reducing endpoint complexity and enhancing internal participant alignment. Endpoints include medical devices, mobile devices, laptops, desktops, servers, and other examples of the internet of things (IoT). Thus, to implement more effective cybersecurity processes in hospitals, the Infosec personnel must understand the intricacies of cybersecurity in the IT working environment.

Effective and Efficient Cybersecurity

Effective and efficient cybersecurity in hospitals ensures the successful performance of security strategies. Although it is impossible for cybersecurity to be 100% effective, and the healthcare risk is an inevitable new paradigm (Martin et al., 2017), cybersecurity must prove effective and efficient to benefit the IT infrastructure in hospitals. However, stakeholders and hospitals can take practical approaches to defend themselves and reduce the impact of cybercriminal attacks. Moreover, these strategies

can resolve cybersecurity difficulties more effectively than unknowingly following more resources (Evans et al., 2016). The effectiveness of cybersecurity involves more than the adoption of multiple strategies but ensuring the security controls engaged are working to the height of their potential. According to Martin et al. (2017), effective cybersecurity must emerge as a vital element of healthcare infrastructure, support regulation, and the focus of future research strategies. Therefore, high performance of security strategies motivated the increase in stability and reliability of the mechanisms in place to produce satisfaction in the triad of information security, such as confidentiality, integrity, and availability of information.

It is indispensable for hospitals to have ongoing compliance with governing regulations. The National Institute of Standards and Technology (NIST) is a non-regulatory agency and a physical sciences laboratory of the United States Department of Commerce (Mansfield et al., 2015). The reality of external audits triggered hospitals to initiate and follow some cybersecurity standards such as the NIST 800-66, which are control objectives for information and related technologies, and information technology infrastructure library (Jalali & Kaiser, 2018). Hospitals are expected to comply with the Federal Information Security Management Act (FISMA) and NIST requirements. These organizations are frameworks assisting in protecting data, operational information, and assets against threats, including cybersecurity breaches.

Hospitals pose a tremendous challenge in fulfilling cybersecurity requirements due to the complexity and lack of resources. For instance, the healthcare industry is fragmented, complex, and unceasingly deficient in resources; nonetheless, it possesses a

tremendous volume of valuable and sensitive data in vulnerable systems (Martin et al., 2017). In contrast, Jalali and Kaiser (2018) claimed that within this massive hospital infrastructure, reducing disparity in resource availability causes the entire healthcare system to be less vulnerable; furthermore, a few hospitals with low resources for cybersecurity threaten the whole healthcare infrastructure. Hospitals must join forces to make the healthcare industry a deterrent to cybercriminals. Singh and Sittig (2015) agreed that the characteristics of hospitals IT (the complex and multifaceted milieu) and related risks management demanded the collaboration of multiple stakeholders, such as patient cybersecurity professionals, healthcare providers, and electronic health records (EHR) vendors, to co-operatively tackle safety problems and develop techniques and strategies to optimize the security of hospitals IT. Hospitals are an exceptionally complex industry with complicated infrastructures, such as diverse technology infrastructure, internal policy, government regulations, and patient care philosophy that demands viable solutions.

Prevention, Detection, and Recovery

The cybersecurity strategies adhered to specific best practices procedures, such as prevention, detection, and recovery. Hence, any data security strategy follows three consecutive steps: prevention, detection, and recovery (Haraty et al., 2018). The first procedure is prevention, which uses many approaches such as firewalls, two-factor authentication, authorization, patching, antiviruses, and other first-line defense. The non-existence of 100% prevention happened because malware can always breach a system prompting the second step, the intrusion detection system (IDS) (Haraty et al., 2018).

Ben-Asher and Gonzalez (2015) indicated that as opposed to novice groups, expert groups of IT professionals meticulously monitoring IDS because they have advanced knowledge and experience in cybersecurity and network operations. Moreover, well-trained operators with exceptional skills in detecting cybersecurity threats are required to supervising the IDS. Also, IDS can detect specific sets of malicious events (Haraty et al., 2018). Finally, discovering cybersecurity threats prompted the third step, the damage assessment and recovery step. Therefore, Haraty et al. (2018) pointed out that the third step cleans up the damage from the healthcare database and returns it to its original state. The triple layers of cybersecurity strategies include prevention, detection, and recovery, working together to reduce hospital cybersecurity breaches. Those three technical controls mentioned above of cybersecurity complemented Security, Education, Training, and Awareness (SETA).

Security Education Training and Awareness (SETA)

A robust Security Education Training and Awareness (SETA) strategy provides the healthcare sector with the strength that mitigates or avoid failures in information security technical controls. To illustrate, Lowry et al. (2015) defined organizational SETA proposals as the level to which an organization officially offers its workforces with an awareness of what cybersecurity risks exist in the work milieu, why these threats exist, and how they can more securely involve in work events. Specifically, a SETA program would set the security tone for the employees of hospitals, especially if it made part of the employee orientation. Similarly, Mohammed et al. (2015) agreed with Lowry et al. (2015) when they stated that hospitals must continuously ensure that employees, to

nurture a security mindset, are aware of security concerns and their specific roles in minimizing and mitigating risks. Consequently, the reduction of cybersecurity breaches in the hospitals must incorporate SETA for the hospital staff. Chen et al. (2015) advocated that SETA program awareness has significant effects on security culture and employees' knowledge of organizational; security policy and that the perception of security monitoring also influences security culture. The InfoSec discipline holds that the human factor is the weakest link in a cybersecurity chain (Anwar et al., 2017). In contrast, Chen et al. (2015) argued that rather than considering employees as the worst problem of information security and utilizing monitoring to control them, they stipulated that organizations should involve employees in the development and implementation of monitoring schemes so that feedback on security policy compliance could help foster a positive security culture. While Anwar et al. (2017) advocated that the human factor is the weakest link in the chain of cybersecurity link, Chen et al. (2015) disagreed and instead proposed the involvement of employees from the planning stage to implementation. Consequently, Boehmer et al. (2015) concluded that the average user could be persuaded to take a more active role in cybersecurity. Therefore, enhancing users' responsibilities for overall cybersecurity in hospitals is a reachable goal, and the Internet can be a treasured tool to promote it.

Vet Third-Party Vendors

Vetting of third-party vendors in hospitals might involve examining if they have penetrating testing, use secure coding techniques, and how implement cybersecurity. Esteves et al. (2017) revealed that in 2013 at Target Corp., a merchant based in

Minneapolis, Minnesota, hackers penetrated the company's network using a stolen username and password from a third-party vendor who provided air-conditioning services. The Target experience provides an understanding of what third-party vendors are doing within the hospitals' environment, such as how they are behaving around high-value assets such as IT systems, the physical computing environment, and PII. Similarly, Mansfield-Devine (2017) agreed that organizations must evaluate collaboration with third-party vendors, such as how they make remote connections to the system network and whether they performed due diligence in disabling default credentials and securing those servers. Before giving access to third-party suppliers to the hospital's IT infrastructure, it is significant to understand how they view and address cybersecurity. Furthermore, Mohammed (2017) stipulated that the healthcare sector must tackle the concern of cybersecurity in a concerted effort because PHI is shared amongst healthcare businesses due to third-party vendors' associations. Therefore, third-party vendors complicate the work of cybersecurity by adding another opportunity for cyberattacks. For example, healthcare institutions or EHR software companies may host meetings using third-party software, and hackers can access these meetings because most systems do not check if the person listed is who they are (Webb & Dayal, 2017). To this end, hospitals should vet every person, especially if they are from a third-party vendor, who attend their online meeting to ensure their identity.

Known Areas of Improvement of Cybersecurity

The significance of the areas of improvement for hospitals' cybersecurity demonstrated the diverse need to have updated best practices to defend against

cyberattacks and security breaches. For example, Blake et al. (2017) explored data breaches in healthcare grounded on the origins of breaches, financial effect, and governmental directives while they recommended improvement tactics focused on prevention, detection, and mitigation. Formulating robust data management strategies for first-time cyberattacks on hospitals' confidential information promotes the stability of the healthcare sector. In their studies, He and Johnson (2015) identified the need to improve learning from incidents and to share security knowledge to prevent future attacks. Information sharing and learning from the wealth of experiences gained from the recent security breaches positioned healthcare InfoSec to improve its defense strategies. Moreover, healthcare, similar to other industries, ought to experience serious reform to improve cybersecurity (Zandona & Thompson, 2017). The reform requires going beyond compliance by adopting a strategic framework for promoting InfoSec in hospitals. Furthermore, as hospitals and healthcare systems endeavor to improve their defenses against cyberattacks, more hackers may perceive public health as a soft target (Krisberg, 2017). Knowing that hackers see hospitals as very vulnerable motivates IT professionals to improve cybersecurity defense. Therefore, the healthcare sector requires the development of efficient defense strategies to prevent many different kinds of cyberattacks, such as malware, denial-of-service (DoS) attacks, hacking the data, email bombing, and targeted attacks arising now and then (Miao & Li, 2017). Such cyberattacks undermine the safety and privacy of patients' personally identifiable information and endanger the patient's care.

A Collaboration Between Government and Manufacturers

The government and manufacturers are working to improve the security of medical devices and other mobile devices connected to the hospitals' IT infrastructure. For this purpose, industry and governmental agencies are cognizant of the necessity to enhance the cybersecurity of medical devices and networks (Stine et al., 2017). However, while government and manufacturers collaborate to improve the security of medical devices, the healthcare organizations are responsible for managing IT upgrades of their equipment, procedures, devices, and facilities without understanding the threat (Fu, 2011). Similarly, Baranchuk et al. (2018) outlined of the capability to improve cybersecurity from the position of the government, manufacturer, patient, physician, and professional societies. Therefore, the combination of government legislation and the manufacturers' technical control strengthened the cybersecurity of medical devices.

User Two-Factor Authentication. In the healthcare industry, the mantra, something one has and something one knows, forms the two elements of two-factor authentication (Eldefrawy et al., 2012). Password authentication plus a smart card is one of the most appropriate and effective two-factor authentication elements in distributed systems (Wang et al., 2015). For several years, safe and privacy-preserving user authentication techniques emerged as a central part of the software of the healthcare IT systems (Islam et al., 2015). User authentication enhanced the security of healthcare IT infrastructure. Wright et al. (2016) claimed that two-factor authentication is the most significant step that users can use to reduce the risk of harm caused by phishing. They clarified that with two-factor authentication, users must deliver an additional authentication factor besides their password, such as a biometric, for example, a pupil

recognition or a transient numeric code generated by an application or device or sent to the user's phone via text message. In contrast, Kogetsu et al. (2018) considered biometrics problems of biometrics and recommended two-factor authentication without biometrics as a viable solution. A different proposal is a secure and efficient radio frequency identification (RFID) tag authentication protocol to overcome security flaws and improve the system efficiency of two-factor authentication (Li et al., 2015). As a result, two-factor authentication requires the user to have some hardware device and know something. Having a USB security thumb drive or software code and a user's password, the user had the required two-factor authentication elements to gain access to the hospital IT infrastructure.

One of the trending components of healthcare institutions is the telecare medical information systems (TMISs), which enable patients to receive medical services in the comfort of their homes To illustrate, Xiong et al. (2017) asserted that the telecare medical information system (TMIS) allowed end-users to access remote medical information or medical services and security, such as privacy protection and authentication of users. Moreover, the TMIS required secure networking and communication to preserve the users' confidential information. Furthermore, efficient authentication is a precondition to guarantee privacy and security in TMIS (Chaudhry et al., 2015). Consequently, during remote access, both the validity of the patients and TMIS computer systems verified authentication. Accordingly, Kennedy and Olmsted (2017) confirmed that user authentication is the first building block for any secure cooperative computing system. They further stipulated that security concerns are on the rise in all areas of the industry,

such as banks and healthcare institutions. Lately, many two-factor authentication schemes have been proposed to introduce an effective mechanism to protect both users and servers (Xiong et al., 2016). Specifically, Li et al. (2016) reported that to improve the security level of authentication schemes for E-health care applications, such as TMIS, a strong user authentication structure with privacy protection is proposed for E-health care systems. Still, the TMIS is a novel application. Therefore, another known area of improvement of cybersecurity in hospitals is the combination of TMIS and two-factor authentication.

System Update

System update or software patching means adding software codes that stop the vulnerability of a software program, hence, improving the security of the IT environment. For this reason, Kim (2018) claimed that if more departments and end-users frequently update their IT systems, the cybercriminal will hack fewer healthcare organizations. System update involves the upgrade of system or application software with computer codes that will enhance the security of the IT system. The best practices for preventing a worm, ransomware, Trojan, or malware infection of several operating systems involve maintaining the system up to date with updates and software patches (Moses & Korah, 2015). Therefore, medical vendors should ship their computerized products with the most updated operating systems to prevent cybersecurity threats to the hospital's IT environment.

Data Backup. One known area of cybersecurity improvement in a hospital is data backup to combat ransomware. For instance, Jarrett (2017) stipulated that ransomware

can confiscate substantial data files, making patient care tough for a long time. Although ransomware encrypts data on an infected computer, it holds the key to decrypting the data until the victim pays a ransom (Richardson & North, 2017). Consequently, the prevalence of ransomware motivated hospitals to ensure successful daily data backups. Accordingly, once the malware attack of ransomware is launched, hospitals have three options: (a) attempt to restore their data from backup; (b) pay the ransom; or (c) lose their data (Sittig & Singh, 2015). Most cybersecurity researchers agreed that making the payment is most comfortable because the hackers need to fulfill their promise to stay in business, and paying involves the least turnaround time for the resumption of operation. While a reliable backup strategy is one of the best practices of hospitals and end-users, the increasing number of paying victims in recent years begged the question that new defense approaches that reduce the damaging impact of ransomware attacks are needed (Kharraz et al., 2018). For this reason, data backup and recovery form only part of a holistic culture to reduce cybersecurity breaches in hospitals. Moreover, the frequent malware attacks and the news ransomware generate crushed the impression that hospitals have daily backups and do an exceptional job of protecting their computerized data (Richardson & North, 2017). However, the most reliable improvement of data protection makes it imperative for hospitals always to have restorable data backups because the real test of backup is the restoration of data.

Security Education Training Awareness (SETA)

Another area of improvement for cybersecurity in hospitals is security education training awareness (SETA). Consequently, Lowry et al. (2015) defined structural SETA

projects as the level to which an organization aptly offers its workforces with an awareness of what threats exist in the employment facilities, the reasons these threats exist, and how they can more securely participate in work undertakings. Moreover, a SETA program sets the security tone for the employees of an organization, especially if it is part of the employee orientation. However, Furnell and Vasileiou (2017) claimed that based on evidence, it is understandable that security awareness and education remain an area wherein many organizations are deficient and are suffering consequently. The central issue addressed here is the necessity of SETA as a viable countermeasure to reduce hospital cybersecurity breaches.

Transition and Summary

In this section, I discussed literature on information security theory and strategies within the context of reducing breaches of cybersecurity breaches in hospitals. Notably, RAT proposed the framework that advanced a conceptual model for this investigation. Furthermore, the study has discussed RAT, ransomware, security strategies, data breach reduction, hospitals' sensitive data, cybercrime and security, end-user training and awareness, and phishing threats to end-user. The following section presents the methodology employed to gather and analyze data responding to the research question.

The primary purpose of Section 2 is to inform the readers of the study's understanding and the research's content. In Section 2, I discussed the purpose of the study; I described the role of researcher, participants in the study, collection of data, and instrument. In addition, I outlined the methodology and its justification and discussed the research ethics and the components of reliability and validity. Section 3 entails the

analytic findings of the study, unearthing themes relating to strategies for reducing cybersecurity breaches in hospitals.

Section 2: The Project

In this section, I discuss the methodology I used to accomplish this study. I start by stating the purpose of this research; continue by addressing my role as the researcher, the research methods and design, the population and sample, the ethics associated with the research, the data collection instruments, the data collection technique, and data analysis and reliability; and finally list the validity underpinnings of this research.

Purpose Statement

The purpose of this qualitative, multiple-case study was to explore the strategies utilized by hospital IT security managers to reduce cybersecurity breaches associated with sensitive data. The research population consisted of IT security managers from three medium-sized hospitals in the eastern region of the United States with cybersecurity strategies to protect against breaches associated with sensitive data. The conclusions from this study may benefit information security practice by increasing the overall understanding of the complex nature of internal and external threats and breaches and the strategies utilized to combat such threats. Consequently, as a result of increased protection of users' private data, the findings from this study may contribute to positive social change by reducing patient concerns related to potential identity theft.

Role of the Researcher

For this multiple case qualitative study, I was the primary data collection instrument. In a study such as this one, the researcher is the primary individual who collects data and develops an understanding of the objectively collected information (Tomkinson, 2014). In this study, my role as the primary researcher in the data collection

process allowed me to collect, organize, and interpret the data. Between 1994 and 2005, I worked as a system engineer for the IT department of a hospital. During that period, cybersecurity threats were at a minimal level because each department ran in an isolated on-premises environment. Despite the disadvantages associated with the compartmentalization of the IT environments, the key advantage was reduced exposure to cyberspace. Kallio et al. (2016) discussed the significance of data collection, and they depicted the role of the researcher as a principal intermediary. Young et al. (2016) examined the extensive use of interview techniques in research to expose the inherent personal bias of the researcher(s), and they stipulated the benefit of using a semistructured approach to mitigate personal bias by using an interview protocol (see Appendix C). Conducting an interview demands a balanced combination of several elements, such as pertinent questions, proper tools, and the milieu (Grenier & Dudzinska-Przesmitzki, 2015). Although my technical skills and engineering capability are beneficiaries, I am not an expert in hospitals' cybersecurity breaches. Even though I collected data through interviews and archived data, I did not have a bias to influence how I interpreted the information or how I collected the archived data. Therefore, in this study, my role included obtaining the participants, conducting interviews to collect data, and analyzing my findings.

Following the interview protocol (Appendix C), I used voice recording and transcription of interviews to capture the data that the participants shared in this study. According to Baur et al. (2015), the lack of full disclosure, which differentiate what personal stakes or inclinations reflected in research, is hard and to show how being

transparent alone are inadequate to mitigate bias. According to the interview protocol (Appendix C), I had no close affinity with the potential research participants. I chose not to study an InfoSec department of any of the hospitals where I previously or currently worked.

I identified the suitable units of analysis and collected data from the research participants through semistructured interviews and documentation. According to Pezalla et al. (2012), the potential exists for a researcher to influence the data collection process as a human instrument in semistructured qualitative interviews. *Bracketing* is a method used in qualitative research to mitigate the effects of presumptions of the researcher and participants that may weigh on the research process and outcome (Tufford & Newman, 2012). Mind mapping involves creating a brainstormed diagram of concepts, and their connections may develop nonjudgmental research findings (Sorsa et al., 2015). I used the listed term(s) derived from bracketing as the new central concept(s), displaying the connections that repeat or that appear most prominent. Bracketing augments scientific rigor and validity in any qualitative study (Sorsa et al., 2015). I viewed bracketing as an ethical imperative that I performed thoughtfully and thoroughly. Therefore, with the disclosure mentioned above, I formulated the research question, qualitative questions, and interview questions, and I applied bracketing as explained above to mitigate the likely influences of the interview protocol.

The Belmont Report addresses questions of ethical interactions with human subjects while doing research and focuses on the fundamental ethical principles of respect for individuals, beneficence, and justice during a study (U.S. Department of Health

Services, 1979). I utilized the outlined principles of the Belmont Report to inform this study relating to informed consent, assessment of benefits and risks, and selection of participants. I adopted a semistructured interview protocol (Appendix C) to formulate the interview questions along with the eligibility criteria for the selection of volunteer participants. Cugini (2015) stipulated that researchers are required to make sense of ethical standards to suitably address the needs of human subjects. The ethical standards outlined in the Belmont Report and the successful precedence accomplished by using those standards to establish a strong structure for research have protected society over the years (Califf & Sugarman, 2015). I followed the principles delineated in the Belmont Report.

Participants

The participants' eligibility criteria included being IT security managers of InfoSec or IT departments of hospitals cooperating in the multiple case study. The eligibility criteria for choosing the participants for this study specified an IT manager who (a) had implemented cybersecurity strategies that might minimize breaches of a hospital's sensitive, confidential, and private data; (b) continuously monitored the IT environment to detect threats to cybersecurity; and (c) was responsible for protecting a hospital’s computers, networks, and data against malicious hackers’ attacks, computer viruses, and security breaches. Gaining access to participants constitutes a significant feature of research because data collection represents evidence to establish credible research (Elo et al., 2014). In qualitative research, the participants’ experience with the phenomenon of interest provides an excellent criterion for their selection (Palinkas et al.,

2015). Likewise, to ensure credibility, sufficient samples are required in research (Galvin, 2015). This study included interviews with IT security managers to create or provide information on strategies to reduce cybersecurity breaches in hospitals. The participants' job titles needed to identify them as hospitals' IT security managers. The participants were IT managers with intimate knowledge of strategies that reduced cybersecurity breaches in hospitals.

To collect data from the hospitals, I reached out to the gatekeeper, the human resources manager of IT, of each cooperating hospital. The midsize category of hospitals has a number of beds between 301 and 700 (Schochow et al., 2015). I identified the midsized hospitals in the eastern United States (New York, Maryland, and Florida) based on the criteria that they met the bed capacity requirement and they had strategies for the reduction of cybersecurity breaches. Gatekeepers are stakeholders of a hospital who can help in gaining access to qualified research participants (Peticca-Harris et al., 2016). The gatekeeper provided me with contact information for the IT security managers employed by each hospital. Perusing the eligibility criteria of the study, the gatekeeper identified potential participants (Boblin et al., 2013). The gatekeeper assisted me in gaining access to the hospital's documents.

With the guidance of the gatekeeper, I contacted the participants via email. The gatekeeper guaranteed my access to the participants (Peticca-Harris et al., 2016). Although the gatekeepers assisted with gaining access to potential participants, they did not ensure that participants collaborated with me (McFadyen & Rankin, 2016). I sent invitation emails (see Appendix B) to the prospective research participants at the hospital

to request voluntary participation in the study. The email included the informed consent form to ensure confidentiality.

My goal was to acquire quality and reliable research data from IT security managers. To obtain unbiased and dependable research data from research participants, Swauger (2011) highlighted the significance of researchers fostering working relationships with participants. After the research participants responded with the stipulated signed informed consent forms (see Appendix C) in endorsement emails, I followed the ethic-of-care method by Swauger through consistent communication with the participants by phone and email to establish a working relationship. I conducted multiple interviews: the initial interview and one or more member checking interviews. I used the interview questions outlined in Section 1 to conduct the initial 1-hour interview, following the interview protocol. The follow-up interview was intended to confirm the interpretation of participants' prior interview responses, as well as the completeness of their previous responses. I was professional with the participants when discussing the possible times to schedule an interview. Moreover, I was transparent about my intents when determining the working relationship with the participants, as outlined by Rubin and Rubin (2011) and Swauger, to guarantee that the participants provided insight aligned to the overarching research question during the interviews. I was not coercive or manipulative in my interactions with the participants. I ensured that the participants understood that they could withdraw at any time during the research process, as noted by Swauger. The participants were at liberty to exercise their free will.

Research Method and Design

I chose the qualitative research method and the exploratory multiple-case study design to address the IT problem and the primary research question. Regarding the viable research methods and research designs, the qualitative method and multiple-case design were suitable to fulfill the research purpose.

Method

I investigated the research methods suitable for this study before I selected a research method. Qualitative, quantitative, and mixed methods are the three viable and well-established methodologies (McCusker & Gunaydin, 2015). Although all three methods are workable for research, the qualitative method contributed a deeper understanding of the research issue (Palinkas et al., 2014). Qualitative research is relevant for exploratory research and triggers further research on a broader scale (Cronin, 2014). Because it facilitated more investigation of the significant aspects of my research, the qualitative method was used instead of quantitative and mixed methods. A researcher can utilize the qualitative research method to delve into each participant's experience (Grossoehme, 2014). Using the qualitative research method to answer the research question, I explored the experiences and personal perspectives of the participants. With the qualitative method, researchers can transfer implications that emerge from the qualitative technique (Alshamaila et al., 2013). Hence, the qualitative method assisted me in gathering information with the purpose of answering the research question. Moreover, qualitative research enables researchers to utilize open-ended interview questions offering participants an opportunity to provide in-depth feedback (Frels & Onwuegbuzie,

2013). When a participant's feedback indicated a need for more information or explanation, I followed through with more probing questions. According to Sarma (2015), the acuity related to rigor in qualitative research is a stereotyped concept spawned from looking at the inadequately supported works of qualitative researchers. Research supports that qualitative research is thorough and reliable.

In reviewing the quantitative research method, I rejected its use for this study because it involves expressing in numbers, confirming theories, and testing assumptions. Quantitative research entails strategies of inquiry, such as experiments and surveys, and the collection of data on fixed instruments that generate statistical data (Purohit & Singh, 2013). My research on strategies for the reduction of cybersecurity breaches in hospitals, however, did not necessitate quantification. Moreover, quantitative research is social research employing the empirical method and empirical statements (McCusker & Gunaydin, 2015). Such numerical data, lacking in-depth explanations of the study's phenomenon, would have failed to provide participants' insights about strategies utilized to reduce cybersecurity breaches. Likewise, quantitative research allows researchers to test predetermined hypotheses (Haegele & Hodge, 2015). The quantitative research method was unsuitable because the focus of my study was not testing hypotheses. Consequently, I declined to use quantitative research for this study because I was uninterested in testing hypotheses or applying numerical measurement to corroborate data. I acquired in-depth research data from the IT leaders by posing "how," "why," and "what" questions instead of using quantitative data collection methods (e.g., yes-and-no survey inquiries).

The mixed method, a combination of quantitative and qualitative research methods, was considered as an option for conducting this study because it provides strengths of both methods. The mixed method is suitable for research demanding an in-depth analysis of qualitative data and multivariate analysis of quantitative data (McCusker & Gunaydin, 2015). When neither a quantitative nor a qualitative method is adequate by itself to understand the research purpose, a mixed-method approach is recommended. However, the quantification of data was not needed in this study to answer my research question. Consequently, I dismissed the choice of both quantitative and mixed methods approaches for this research. Furthermore, the mixed method involves an up-close exploration of a phenomenon and validating the findings to identify the relationship that addresses a research question (Farrelly, 2012). Regarding the mixed-method research methodology, I did not choose this method because it would not have fulfilled the projected purpose of the study, which was to focus on exploring the IT phenomenon.

Research Design

Of the four viable qualitative research designs, namely phenomenology, case study, ethnography, and narrative, I chose an exploratory multiple-case study because of its suitability to achieve the purpose of the study. Palinkas et al. (2014) outlined four qualitative design types (i.e., phenomenology, ethnography, narrative research, and case study). Raeburn et al. (2015) classified case study design as a flexible research design to enlighten, explain, or understand phenomena in their everyday context. From the viewpoint of those who experienced a phenomenon, case studies offer a holistic

comprehension of a phenomenon within real-life milieus (Stake, 1995). A qualitative exploratory multiple-case study was suitable for this research because it allowed for an in-depth understanding of hospital IT security leaders' perspective on strategies for the reduction of cybersecurity breaches in hospitals. The primary purpose of this study was exploring strategies to reduce cybersecurity breaches in hospitals; therefore, the multiple-case study design was appropriate for this study.

The multiple-case study design can incorporate "what," "how," and "why" questions in semistructured interviews coupled with review of a hospital's documents to achieve an in-depth understanding of a phenomenon. According to Cronin (2014), case study research answers "how" and "why" questions regarding phenomena. The analysis of hospital documents corroborated the interviews and heightened my understanding of the strategies utilized to reduce cybersecurity breaches in hospitals. Moreover, Ketokivi and Choi (2014) argued that a case study design promotes diverse data sources and allows for the exploration of phenomena within an existing context. Likewise, in this study, the collection of data came from various sources such as semistructured interviews, existing literature review, and gathered hospital documents. Therefore, I selected the multiple-case study as the most appropriate qualitative design for exploring strategies for the reduction of cybersecurity breaches in hospitals.

I considered the phenomenology research design for my study. According to Moustakas (1994), phenomenology research design involves lived experiences and events related to a phenomenon. Grossoehme (2014) stipulated that phenomenology research zeroes in on participants' experiences and the meaning of the experiences. Participants'

experiences were necessary for my study; however, a phenomenology research design would have prevented my collection of hospital documents from providing findings on the hospital's viewpoints. Gill (2014) stipulated that qualitative researchers develop and use phenomenological research design to scrutinize individuals' experiences. Phenomenological design lacks the level of flexibility of a case study (Hyett et al., 2014). Although phenomenological design may be used to explain an individual experience, my study required the flexible qualitative data collection method offered by case study design. Therefore, I declined to use the phenomenology design because it was misaligned with my research question.

For this study, I considered ethnography qualitative design as a viable option. Researchers intending to acquire an in-depth comprehension of a culture utilize an ethnographic design (Murthy, 2013). Ethnography emphasizes a protracted cultural inspection, which was not the focus of this study. Cruz and Higginbottom (2013) outlined data collection tools of ethnography, including the scrutiny of apt documents, participant inquiry, interviews, and member checking. Moreover, Morse (2015) stipulated that ethnography aligns with the usage of a theoretical framework as opposed to a conceptual framework. My study, however, demands a conceptual framework instead of the theoretical framework, and I am not exploring the cultural phenomena pertinent to my research. I was exploring the strategies for the reduction of cybersecurity breaches in hospitals; therefore, an ethnographic design is inappropriate for my research.

Lastly, I contemplated using a qualitative narrative design for my study. According to Wolgemuth (2014), a narrative study denotes assembling objects and life

experiences for storytelling of the methods human's experience in the world. In contrast, I focused on strategies to reduce cybersecurity breaches in hospitals as opposed to how humans experience the world. Researchers using narrative inquiry must be cognizant of the power bonded relationship resulting from sharing stories without encouraging participants to overshare reluctantly (Berry, 2016). Even though storytelling would provide richness to this study, it would not fulfill the purpose of exploring strategies to reduce cybersecurity breaches in hospitals. Acquiring understanding through listening to individuals' stories, researchers used narrative and storytelling interchangeably (Joyce, 2015). My study focused on hospitals' strategies as opposed to the life experiences of individuals, not producing the appropriate data to answer my research questions. Consequently, a narrative study is inapplicable to my research.

I chose the case study research design as opposed to the other viable qualitative designs (phenomenology, narrative, and ethnography) to guide this study because of its suitability to achieve the purpose of the study (Petty et al., 2012). If the researcher's goal is to comprehend the human experiences about a specific phenomenon, then other qualitative research designs are suitable (Erlingsson & Brysiewicz, 2013). The primary purpose of this study is to explore the strategies to reduce cybersecurity breaches in hospitals. Therefore, the other designs were not suitable for this study.

The multiple-case study design provided me with a broader perspective to extract data on strategies for the reduction of cybersecurity breaches in different hospitals. In contrast, Stewart (2012) argued that a single holistic case in one milieu has more considerable study limitations. However, Campbell and Ahrens (1998) suggested a

multiple-case study provides the replication logic whereby each case is perceived individually. The process of researching multiple examples of the same case in a multiple-case study design promotes my comprehension of the IT problem. The duplication of approaches for each subset in a multiple-case study could enhance the validity and generalizability of the study findings (Zivkovic, 2012). Therefore, multiple-case design involves more than one sample of the same case to find similarities and differences.

Population and Sampling

In this sub-section, I described the population, explained the sampling method, stipulated the sample size, discussed how data saturation was achieved and outlined the setting for the semistructured interviews. In this study, besides my understanding that the hospitals have effective strategies and merit studies, I chose three hospitals based on their relative size and willingness to cooperate. Based on these eligible criteria, each hospital had approximately three IT security managers, resulting in a total population estimated to be approximately nine IT security managers. The gatekeeper provided me with contact information for all of the hospital's IT security managers, which I then used to solicit participation from the population. According to Berger (2015), the population features relate to participants' subjective experiences with the phenomenon within a qualitative study. The IT security managers, who constitute the population of my research, possess skills in the study's phenomenon, and strategies for the reduction of cybersecurity breaches in the hospitals. Malterud et al. (2016) pointed out the purpose of choosing a population for the study is to solicit all possible information with minimal participants.

Consequently, each participant is an experienced and knowledgeable IT manager employing strategies to reduce of cybersecurity breaches in hospitals.

I evaluated two viable purposive sampling techniques for this study: (a) convenience sampling and (b) total population sampling. According to Gentles et al. (2015), purposive sampling is a participant sampling technique to address particular purposes concerning the research questions. Therefore, the concepts of purposive sampling, a non-probability sampling scheme, allowed me to select participants based on the population's characteristics and the study's objective. Singh (2016) explained that convenience sampling collects data from a population whereby the individuals are easily reached and can participate. Convenience sampling refers to a purposive sampling approach that a researcher uses to choose a sample of participants from a population whereby the subjects are close at hand. The drawback of convenience sampling is the increased likelihood that the sample is not representative of the whole population since few participants could inject sample biases into the collected data (Singh, 2016). Consequently, I chose not to use the convenience sampling technique to minimize the potential for sample bias.

I utilized the second option, total population sampling, referred to as a type of purposive sampling, where the researcher studies the whole population of interest. My population consists of IT security managers who work for the three mid-sized hospitals in metro Atlanta. My sample size is estimated to be nine participants based on my estimate of a total population of nine IT security managers. Etikan et al. (2016) denoted total population sampling as a method whereby the entire population meets the criteria such as

particular expertise and experience included in the research. According to Marshall (1996), the total population of possible primary participants is small because the recruiting criteria determined the sampling size that meets the narrowed stipulations. I used total population sampling for all practical purposes because my target group is small and distinguished by selective and well-defined characteristics. Crossman (2020) stipulated that a researcher uses total population sampling to explore the entire population with shared traits. In total population sampling, I explored the entire population since the population size possessed the required characteristics, which resulted in a small sample. The shared uncommon characteristics of the IT security managers resulted in a small population. In this study, I explored the total population of approximately nine IT security managers in the three hospitals to achieve data saturation. Exploring a relatively small number of cases, the researcher commonly used total population sampling (Etikan et al., 2016). Total population sampling is often used where the investigated sample size is reasonably small. Using total population sampling to collect data, the researcher had a higher likelihood of reaching data saturation (Suri, 2011). In total population sampling, data saturation for the entire population is dependent on achieving data saturation with each participant. Although other purposive sampling techniques may continue to sample additional participants until data saturation is achieved, the total population sampling approach must achieve data saturation with the entire population. In this study, the population was small and limited by the eligibility criteria, whereby total population sampling is the most appropriate option to provide a complete and detailed comprehension of the phenomenon.

Data saturation is a methodological principle in qualitative research that indicates that further data collection and analysis are unnecessary. Data saturation is the precise moment in data collection and analysis when new information produces minimal change to the collection of codes (Guest et al., 2006). Data saturation is attained when adequate information to replicate the study and the ability to get additional new information has been achieved and when further coding is no longer achievable (Fusch & Ness, 2015). According to Tran et al. (2016), using purposeful sampling (total population sampling) and in-depth, open-ended questions (semistructured interviews) would provide richer answers per participant and require smaller sample sizes to achieve data saturation. In this study, the entire population restrained by the eligibility characteristics was the source for all my information. The concept of data saturation is easy to comprehend but difficult to establish in practice because it is contingent on the topic, purpose of the research, participants, and the way data is collected (Tran et al.). After considering the purpose of my study with the sampling technique of the entire population narrowed by the study's objectives, I reached data saturation because I included the whole population in my data collection. According to Fusch and Ness (2015), the identifying criteria for data saturation occur when no new information, no new coding, and no new themes stem from interviewing the research participants. After applying these criteria with narrowed objectives (IT security managers' characteristics) to the interviewing of approximately nine research participants, I worked to achieve data saturation. Researchers should critically consider how saturation parameters best influence their study and affect data adequacy (Vasileiou et al., 2018). My study used all the approximately nine IT security

managers of the three hospitals' IT departments; hence, when I finished collecting the in-depth and rich information from each case, I achieved data saturation. Therefore, after I used these testing measures, the approximately nine research participants should be sufficient to attain data saturation.

After I conducted the initial interviews, I performed a follow-up member checking interview to ensure the accuracy of the collected data, data saturation, and the correct interpretation of the data. According to Kornbluh (2015), member checking denotes a validation technique, while Birt et al. (2016) stipulated that member checking helps investigate wherein results resonate with the participants' viewpoints. I used member checking to ensure the accuracy of the interviews by reviewing the information gathered from the participants from the initial interviews. Fusch and Ness (2015) explained the member checking process as conducting the initial interview, interpreting what the participant shared, and sharing the interpretation with the participant for validation. Member checking and follow-up conversation, which is a proven tactic where I approached the participants to verify my interpretation of their interviews. I scheduled a follow-up interview with each participant for about 45 minutes. Naidu and Prose (2018) posit using member checking to guarantee the authenticity of data. Within a week of the initial interviews, I conducted member checking to analyze the information and gravitate towards data saturation. Erlingsson and Brysiewicz (2017) purported the use of member checking can reduce the error rate prior to data analysis, and it promotes study validity. The goal of the member checking session was to allow each participant an opportunity to either confirm or deny the clarification of the data. In a study, the use of member

checking can achieve data saturation, validity, and reliability (Andrasik et al., 2014). Member checking ensured another interview, which helped in confirming data saturation. In qualitative studies, the onus is on the researcher, to decide at what point they reach data saturation (van Rijnsoever, 2017). During the data collection phase of the study, data saturation may result from no new information since the researcher incorporates member checking into the study (Unluer, 2015). In this study, member-checking interviews with each participant bolstered data saturation since each participant was allowed to review and verify my interpretations of the collected data.

Sample size determination is the process of selecting the number of observations or replicates to use for the sampling of the population. According to Boddy (2016), in qualitative research, the determination of sample size is relative and partially contingent upon the scientific paradigm under which the study is happening. Total population sampling determined the sample size of this study. The sample size evolves from the desire to achieve data saturation or generalizability and support variation with the target population (Leech & Onwuegbuzie, 2007). Three primary references that helped me decide on the sample size of N=9 samples for this study are (a) Boddy (2016); (b) Malterud et al. (2016); and (c) de Bekker-Grob et al. (2015).

Ethical Research

Research that engages human beings, participants, raises unique ethical issues, such as the consenting process, allowing the participant to withdraw, offering incentives, maintaining secure data, and declaring agreement documents. Stichler (2014) found that for an ethical research process, a researcher must obey the acceptable agreement, legal

enforcement, and social suitability to contribute valuable knowledge to the branch of learning. The primary elements of ethical research I considered were Institutional Review Board (IRB) approval, informed consent, confidentiality, handling of sensitive data, inducements, and voluntary participation. The IRB is a faculty at educational institutions that reviews research to protect human subjects (Ghooi, 2014). Thus, I got authorization from the Walden University IRB, which endorsed my doctoral study for no threat to research participants. Consequently, after the IRB approved my intended study, they gave me an approval number, 10-25-21-0657176, which I put on the informed consent form I sent to the research participants.

I commenced the data collection process after the IRB approval by contacting InfoSec C-executives at the hospitals by phone and networking with the IT leaders to acquire permission to conduct my study within their health institutions with the assistance of the participants. If the IT C-executives expressed interest, I sent emails that included the letter of cooperation (Appendix A) to acquire permission to interact with the participants. After the IT C-level executives gave me approvals, I sent the invitation emails (see Appendix B) package of informed consent forms to prospective research participants to read, sign, and return. The informed consent form contains information about the study to educate and prompt the research participants to accept the invitation (Tamariz et al., 2013). The participants did not receive any incentive or compensation to contribute to the research. However, I offered the participants a hard copy of the completed study. I advised each participant of the option to decline participation in the study or retract during the interview process without any penalties.

I collected permission from each participant to audio record the interviews. Moreover, I used Microsoft Windows Voice Recorder software to record the interviews. Contingent on the participant's availability and location, I conducted initial face-to-face interviews or utilized Microsoft's Skype application. Then, I followed-up with interviews via telephone. I selected three hospitals from the population of 100 hospitals in Metro Atlanta, Georgia. Each gatekeeper at the three chosen hospitals gave me approximately three participants based on the eligible criteria. Next, I selected the three participants at each hospital. To facilitate the privacy of each participant, I employed alphanumeric codes to label every participant based on the transcribed data from the interview. I coded the participants and hospitals in ascending order of the conducted interviews. Table 2 displays a summary of the intended use of the three interview mechanisms and anonymized participants' information to be used in the interview data for data analysis and the presentation of findings.

Table 2

Interview Mechanisms and Anonymized Participant Information

Interview mechanism	Anonymized hospital	Location	Number of participants	Anonymized participants
In-person Zoom	Hospital-1	Maryland	3	P1, P2, P3
In-person Zoom	Hospital-2	New York	3	P4, P5, P6
In-person Zoom	Hospital-3	Florida	3	P7, P8, P9

American Psychological Association (2010) stipulated that after the completion of the study, the researcher should store the data for five years. The data retention strategy

involved storing the audio recordings and documentation on an external storage device such as a flash drive or a hard drive to prevent public disclosure, misuse, or misinterpretation. I kept the collected interview data in a secure, password-protected, and fire-rated safe for five years, with me having exclusive access. Consequently, at the end of five years, I will destroy the audio-recorded files and shred transcribed interview data, including hospital paper documents given to me by the participants.

Data Collection

Data collection is a process of gathering data for findings and conclusions of the study that stem from thorough data analysis and interpretation by the researcher. In this subsection, I discussed the instruments, the data collection techniques, and the data organization techniques.

Instruments

In this qualitative research, I am the primary data collection instrument. According to Barnham (2015), the researcher is involved in every aspect of the study from the planning stages to its recommendations. Researchers conduct semistructured interviews to pinpoint themes and gather in-depth knowledge and understanding of the phenomenon under consideration (Yeoh & Popovič, 2016). Lim et al. (2012) recommended that a collection of data should comprise two of several sources, such as documents, observation, interviews, physical artifacts, archival records, and participant observation. I used semistructured interview protocol, direct observation field notes, and analysis of hospital security policies and documents.

I used triangulation, whereby the researcher used at least two methods to gather data on the same topic. Denzin (1978) and Patton (1999) identified four types of triangulations: (a) method triangulation, (b) investigator triangulation, (c) theory triangulation, and (d) data source triangulation. Method triangulation encompasses using a minimum of two options to collect data such as questionnaires, documents, interviews, and observations (Murray, 1999). Method triangulation, often used in qualitative research, may consist of interviews, observation, and field notes (Carter et al., 2014). Therefore, in this study, I utilized method triangulations.

Moreover, I used semistructured interviews accompanied by documentation such as the hospital's documents, patient records, and employees' information to ensure methodological triangulation. Methodological triangulation involves using at least two kinds of methods to study a phenomenon (Bekhet & Zauszniewski, 2012). In this study, methodological triangulation aims to enhance my findings' reliability and credibility. Hanson et al. (2011) explained the advantage of utilizing semistructured interview questions in qualitative research, whereby the researcher has the flexibility to adjust the questions as needed to extract all-encompassing data from the participant. To acquire an in-depth understanding of the specific IT problem, I used, when suitable, flexible probing questions along with open-ended interview questions. Furthermore, Jacob and Furgerson (2012) argued that researchers use interview protocols to structure the interview process utilized in obtaining qualitative data. Therefore, I applied the interview protocol (see Appendix C) to increase evenness throughout the semistructured interview activity involving all research participants.

Not only conducting the interview is significant, but the preparation for the interview ensures successful completion. For this paragraph, Valenzuela and Shrivastava (2002) provided the guiding ideas before and during the interview, and I shared pertinent information with each interviewee. Choosing a place without distraction for the interview is ideal, I recommended somewhere away from work, such as a room at the library. Apart from preparing the recording device, such as a smartphone recorder, I take notes in the form of a reflective report. Moreover, I explained the purpose of the interview is to explore in-depth information on the strategies in place to reduce cybersecurity breaches in hospitals. I stipulated the terms of confidentiality to encourage trust. I elucidated to each interviewee the format, a semistructured interview, whereby open-ended questions trigger discussion, and I followed up with probing questions. Each interviewee knew the length of the initial interview as one hour, and not only I follow up with one member-checking interview of the less time each. I provided my contact information to each interviewee. Finally, I facilitated each interviewee to make clear any doubt relating to his or her interview.

I began each interview with a qualification conversation to ensure that I spoke with the appropriate person. I used relaxing questions to help the participant feel unthreatened yet generate an interactive and fun introduction. Before asking interview questions, I shared with each participant a short overview of the intent of the study, the interview, and the confidentiality guidelines. Kyvik (2013) insisted that the researchers ask the ten semistructured interview open-ended questions (see Appendix D) based on the IT problem under consideration to each participant in a logical order to diminish bias.

Hence, following the interview protocol, I provided the same order of interview questions to stimulate a similar trend of thought among the participants of the interviews. I took notes and clarified the participants' nonverbal communication, such as body language, gestures, tone of voice, and facial expressions. When necessary, I asked probing questions to ensure the participants provided detailed responses to the interview questions. I monitored the interview time to ensure the research participants provided sufficient research data to the interview questions. I ended the interview by expressing my gratitude to the participants for their time and informing them of the follow-up interview after their first in-person or Skype face-to-face interview.

Although documents may be used as a single tool for data collection and analysis, gathering the pertinent hospital documents requires the collaboration of the gatekeeper, each participant, and myself. Collected documentation augments what the researchers use to develop their awareness of the research topic and maintain other qualitative data sources (Bowen, 2009). I obtained IT hospitals' documents such as security policies and procedures, logs for information security events, information security workbooks, data users' roles and responsibilities, and SETA programs. Moreover, I extracted archival documents such as security logs and incident reports. Furthermore, I intend to get public domain information, such as minutes of security meetings and press releases scripts, the hospitals' websites, health industry publications, and other public sources. I used relevant keywords to search hospitals' IT environment's public domain. While interviewing the participants, I requested them to share documentation about the research theme via email to support their responses and my comprehension of the IT problem. To corroborate the

data collected from interviewing the research participants, I used the documented information pertinent to the research topic.

Member-checking, also referred to as respondent or participant validation, is a procedure for exploring the credibility of the data collected from the semistructured interview and documentation. Harper and Cole (2012) argued that member checking is a quality assurance process researchers utilize in qualitative research to improve the validity and precision of the collected data from the respective interviews. Following each interview, I summarized the responses to each question that I extracted from the transcribed data of each research participant. I interpreted the summaries to garner an understanding of what the participants communicated. Before the scheduled follow-up interviews, I provided each research participant with a copy of the interpretation of my summary of his or her transcribed interview data. During the follow-up interviews, I requested the participants to corroborate the information for correctness. I asked the participants, where necessary, to provide changes or the addition of missing data. After the follow-up interviews with the participants, I made any suitable changes to my digests and clarifications of the transcribed data as deemed necessary. In this study, I used member checking to assist with the improvement of the reliability and validity of the data collection instruments.

Data Collection Technique

The face-to-face interview, also referred to as an in-person interview, is a data collection technique where the interviewer directly communicates with the participant while using semistructured questions. According to Peters and Halcomb (2015),

semistructured interviews are a common approach of data collection in which the interviewer (researcher) poses predefined questions but then probes further as the participant responds to produce reliable data that provide insights into the participant's perceptions. Although Trier-Bieniek (2012) portrayed telephone interviews as a more time-efficient and researcher-friendly technique for conducting interviews, I used the face-to-face semistructured interview as the primary data collection technique for this study to gather research data from participants at the first interview. My reasons for choosing an in-person interview versus a telephone interview are that it provides accurate screening, captures both verbal and non-verbal cues, keeps focus, and captures emotions and behaviors. Furthermore, I performed the follow-up interviews via telephone while utilizing a semistructured format. I followed the interview protocol (see Appendix C) as the template for conducting the semistructured interviews. I performed three sets of three remote interviews with the chosen three hospitals in the eastern United States.

I scheduled the first semistructured in-person interviews at an appropriate time, date, and place that both the participants and I agreed on. I scheduled the in-person interview for first interviews at a public location and at appropriate times that coincide with the participant's non-work schedule. According to Lo Iacono et al. (2016), researchers can use Skype virtual face-to-face interviews as another choice or in addition to the regular face-to-face interview. If I use Skype face-to-face interviews, then I set up the interviews at apt times separate from the participants' work schedules. For the follow-up interviews, I arranged telephone interviews at convenient times in alignment with the participants' non-work time. Petty et al. (2012) stipulated that those researchers usually

use 30 to 90 minutes to complete qualitative research interviews. In this study, I limited the time of interviews just to a one-hour increment.

To achieve an effective and efficient interview meeting in accordance with the interview protocol (see Appendix C), I implemented the following procedures: (a) ensure the interview question is clear, (b) prepare a checklist of the interview questions (c) communicate the precise purpose of the interview session, (d) begin with qualification questions to trigger a comfortable atmosphere, (e) use open-ended interview questions to stimulate the choice of the participant's response, (f) formulate each question with just a single idea, and (g) summarize the answers provided by the participants. Ranney et al. (2015) recommended the using audio or video recorders to document qualitative interviews to acquire research data quality. While conducting the interview, I used Microsoft Windows Voice Recorder to collect the data for reliable data transcription.

Via the signed informed consent documents, I received permission to audiotape the interview. Moreover, before I began the interview, I asked the participants for approval. Coupled with the audiotaping, I take notes during both the in-person and telephone interviews. Researchers can use a data collection technique known as documentation, which is existing information about the research topic (Hanson et al., 2011). I corroborated data collected from the interviews with documentation from the hospital's documents. Examples of such documents are information security policies and procedures, archival records, or public information to conduct data analysis and answer the research question.

After I shall have reviewed their policy, I employed the TranscriptionPuppy company's 24-hour turnaround service to transcribe the interviews' digital audio files to text in the Microsoft Word app. Walden University IRB requires a doctoral candidate to procure a confidentiality agreement from any person or company before allowing them to review the research data. The quality control and privacy policy (see Appendix E) of TranscriptionPuppy clearly states that before accessing and transcribing the digital audio or video file, the organization provides the customer with a signed non-disclosure agreement. After I acquire the transcribed data from TranscriptionPuppy for each interview, I used the ATLAS.ti software application to perform analysis to attain an understanding of the respondents' information. Research respondents received a hard copy of the analyzed data of their respective interviews before the scheduled follow-up interview. I asked each respondent to cross-check the information and implement any necessary changes. I made all suitable changes to my summaries and interpretations of the transcribed data after the follow-up interview with the respondent. Performing the member checking method enabled me to validate the reliability of the research data I used for data analysis, thereby improving the validity of the research findings.

The advantages of the in-person semistructured interview include the opportunity to glean more valid information about informants' mindsets, standards, and opinions, especially how the participants elucidate and contextualize their answers. According to Stoop et al. (2012), the advantage of in-person semistructured interviews is the ability of the researcher to build understanding, trust, and relationship with the informant to improve engagement and response quality. In contrast, researchers use Skype interviews

instead of in-person interviews to minimize travel expenses and accommodation (Lo Iacono et al., 2016). In spite of the advantages of the in-person interview, it may be necessary to utilize Skype interviews instead of face-to-face interviews to combat the disadvantages of in-person interviews. Moreover, the benefits of conducting semistructured telephone interviews for follow-up interviews are that it minimizes expenses, maximizes time-saving, stabilizes mentality, and capitalizes on the availability of the participants (Rapp et al., 2012). However, a disadvantage of the telephone interview as a data collection approach is the inability to capture the body language of the informant (Wright & Ogbuehi, 2014). Even though the disadvantage mentioned above is cognizance of semistructured telephone interviews, such interviews are a viable option for data collection techniques for in-person interviews. Furthermore, the research finding of Rapp et al. was that in-person and telephone interviews combination could provide similar results from informants.

While conducting the interviews, I solicited the hospital's documents, archival records, and public information. The pertinent hospital documents included IT security policies and procedures; the archival records consisted of security incidents reports; the general information may be found on the Internet and other public domains. The participants emailed such documentation, which was used to corroborate their responses and enhance my understanding of the IT security problem. As mentioned above, I examined the data collected from the documentation, to answer the research question. Moreover, I conducted searches on the Internet or in healthcare industry publications on the strategies that reduce cybersecurity breaches in hospitals. Using keywords such as

cybersecurity and hospitals, hospitals and ransomware, and *hospitals and phishing,* I performed internet searches. I focused the findings from the public domain on their relevance to my study's topic. Consequently, I conducted methodological triangulation by integrating documentation collected from the informants, the public domain, and interview data.

Data collection technique, namely documentation, triggers triangulation wherein more than one method to collect data on the same topic assures the validity of the research. Likewise, the benefit of documentation provides the researcher with qualitative data to comprehend the context of the research topic and validate the information from additional data sources (Bowen, 2009). The documentation, compared to interviewed data and observation of participants, is more accessible and cost-effective (Hanson et al., 2011). In contrast, the drawback of data collected from the documentation is the irrelevance to the research topic because the data was generated for unrelated reasons. The primary advantage of acquiring documentation through a data collection technique is that it provides access to information that would otherwise be difficult to glean.

Data Organization Techniques

The researcher understands and analyzes the collected data efficiently because of the practice of reliable and accurate data organization. Researchers use a strategy to achieve anonymity for participants is caused by assigning generic codes to each research participant as a data organization technique (Gibson et al., 2013). I coded the three participants for the first hospital (Hosptial-1) as P1, P2, and P3 with corresponding audiotapes as Audiotape-P1, Audiotape-P2, and Audiotape-P3. Anyan (2013) agreed that

researchers could acquire data integrity by applying organizational techniques to the research data. I organized the collected data, such as documentation from the informants and public information about the healthcare institution, into computer folders (directories). To conduct reflective journaling, I used Microsoft Word and OneNote (Pack, 2014). Every week, I documented my reflection on the research data collected in a reflective journal. Consequently, I kept track of the developing understanding of the research.

The data organization technique for this research requires planning and commitment. Some elements of data organization are electronic folders for storing various data files such as audiotaped interviews, transcribed interviews, reflective journals, researched documentation, and member-checking documents. I used the ATLAS.ti as the data analysis software because it has proven to generate excellent research analysis. Other viable data analysis software includes NVivo, HyperRESEARCH, QSR, and MAXqda; however, I proceeded according to the reviews, which highlighted the user-friendliness and reliability of ATLAS.ti. Paulus and Bennett (2017) recommended the ATLAS.ti software tool to use in qualitative research to conduct content analysis to address a research question. Consequently, I choose ATLAS.ti application as the qualitative tool to perform a content analysis of the interviews and the hospital's documentation data to decide on the themes and achieve understandable information from the data.

The USB flash drive is the storage device for the recorded research interviews, interviewed notes, reflective journals, data transcription, hospital documents, and

additional researched-related documents. Moreover, I used my online Dropbox storage as backup storage for the research elements. Furthermore, a researcher is required to securely retain research data for up to 5 years before disposing of the data (American Psychological Association, 2010). Ye et al. (2018) recommended the protection of the USB flash drive for five years in a locked fire-rated password-protected safe vault to facilitate confidentiality, privacy and avoid abuse of the research data. Walden University requires that all research data be destroyed after five years of completing research. Five years after the completion of the research, I cross-shredded research documents, such as research notes, reflective journals, and hospital documents. Furthermore, I will digitally destroy electronic files, such as transcribed data files and audiotaped files.

Data Analysis Technique

Data analysis aims to extract comprehensive answers to the research question of what strategies are in place to reduce cybersecurity breaches in hospitals. In order to extract such answers, I employed content analysis using ATLAS.ti. The ultimate output of the content analysis is a set of construct maps that delineate the key themes, the relationship across these themes, and the strength in those relationships. The key analytic steps in creating the construct maps are: (a) adding text documents for data collection, (b) creating quotations and assigning codes, (c) distinguishing and reviewing complex codes, and (d) categorizing codes into themes also referred to as extracts, (e) establish a relationship between codes and themes, and (f) report the findings of primary themes.

In this study, three phases of content analysis have been executed that lead to six data analysis steps. Elo et al. (2014) stipulated that the three phases of conducting content

data analysis are preparation, organization, and reporting. The preparation phase (Phase 1) of qualitative content data analysis occurs when a researcher examines the source data to pinpoint the elements of analysis and understand the entire data set (Vaismoradi et al., 2013). The preparation phase contains a single step, here referred to as Step 1, which comprises two sub-steps: (a) identify the quotations within the imported documents for analysis within ATLAS.ti software and (b) study transcribed interview data and documents to gain familiarity with the data set.

In the organization phase (Phase 2), I performed four key steps numbered steps 2 to 5. According to Elo et al. (2014), the initial step of the organization phase includes conducting deductive or open coding, categorizing the codes, and grouping the codes under primary headings. In step 2, I performed the following three sub-steps: (a) generates deductive codes categorized from collected documents into ATLAS.ti software, (b) completes a line-by-line analysis of the triangulated data to explain codes of data such as sentences, clauses, phrases, and words, and (c) summarizes the data by associating codes to the quotations and then grouping the codes. Next, in step 3, I performed two sub-steps: (a) distinguishing the list of all quotations and codes generated from the coding process and (b) using the network view in ATLAS.ti software to review complex code to better grasp how the quotations relate to the codes. After that, in step 4, I executed three data analysis sub-steps: (a) scrutinizing the codes to explore for themes, (b) using the network view in ATLAS.ti to categorize themes patterns to create construct maps in relation to the conceptual framework, and (c) identifies central themes that are relevant to the entire information from the data set and the research. Next, in step 5, I completed five

sub-steps: (a) evaluates the interaction and relationships between codes to verify relation to the primary themes, and (b) using the Code Co-occurrence and Word Cruncher tools in ATLAS.ti software to categorize any unnoticed codes and to analyze code relationships, (c) reiterates assessment of the relationship of codes to categorize likely new developing themes, (d) focuses on primary themes emerging with the data, and (e) compares the categorized central themes with the documents and the conceptual framework.

Finally, the culminating phase of qualitative content data analysis is the reporting phase (Phase 3), which encompasses a single step of reporting the analysis activity and the findings of the primary themes of the documents and conceptual framework. Step 6 is the single step of the reporting phase of content analysis. In step 6, I completed the content data analysis activity by documenting the data analysis process and findings of the relationship of the codes to the categorized key primary themes to answer the research question.

Procedurally, after I received the transcribed interviews from the transcription company, I employed ATLAS.ti, which is a computer-aided qualitative data analysis (CAQDA) software, to complete summaries of the research respondents' answers. ATLAS.ti software requires readable data. I imported the nine interview data transcripts into the ATLAS.ti software. After that, I imported 32 relevant organization documents, and archival records into ATLAS.ti software to generate data analysis. Next, I created quotations (yellow highlighted information), which are a segment from the documents or "chunks of data" (sentences or paragraphs) from the imported abovementioned documents. Following that, I associated codes, which are short phrases, words, or

sentences, with quotations. I used the codes, and tags associated with quotations, to describe or synthesize the imported data. I used codes associated with the quotations to triangulate the imported documents, thereby facilitating the validity of the interview data from participants and understanding of the research question. Table 3 shows the six steps of the data analysis technique and explains each step's what, how, and why. The Step column depicts the "what" feature while the Details column embodies the "how" and "why." In table 3, steps 1, 4, and 5 have two parts to keep the table consistent with the six steps outlined above.

Table 3

ATLAS.ti Data Analysis Techniques

Phase/Step/Substeps	ATLAS.ti execution details (how and why)
Phase 1/Step 1/ Sub-steps a-b. Import the nine transcribed texts of the participants' interviews.	How: "Documents" > "Import Documents". Go to directory Interviews and select the files. Why: The nine documents contain the text used for analysis. For example, interview transcription is considered a document.
Phase 1/Step 1/ Sub-steps a-b. Import the supportive documents such as archive data, policies, and procedures.	How: "Documents" > "Import Document." Go to Supporting Documents directory and select all procedure documents. Why: All supportive documents are salient data to triangulate the interview transcripts. For example, notes taken during the interviews are supportive documents.
Phase 2/Step 2/ Sub-steps a-c. Create quotations, each consisting of a segment or "chunk of text data," such as a paragraph from the interview documents.	How: Highlight or select a segment of text from the interview documents imported in Step 1; right click and "Create Quotations." Such action allows ATLAS.ti to create a list of quotations that can be displayed on the next right panel. Why: Quotations are qualitative data analysis (QDA) elements that trigger distinct interactions with other qualitative elements. The quotations are supporting data relevant to answer the research questions. The quotation: "Cybersecurity, information technology security, or computer security is the protection of computer components from theft or damage" is a typical example of a quotation in ATLAS.ti.

Phase/Step/Substeps	ATLAS.ti execution details (how and why)
Phase 2/Step 3/ Sub-steps a-b. Create codes each of which denotes a word or phrase which identify an interesting feature of the data salient to the research question	How: Highlight quotation in a text document. Next, Click "Codes menu" > "New Code (s)" or "Auto coding." Type the name of code in the pop-up window and click Add. Why: Codes are conceptual constructs representing the essence behind the quotations. Adding such codes to quotations facilitates deductive data analysis. Codes are tags to the quotations. For example, “resources” is a tag for a quotation such as “Resources are often not available.”
Phase 2/Step 4/ Sub-steps a-c. Write Memos or notes associated with codes	How: “Memo” > “New Memo” (Click New memo from the Memo menu). Type the memo. Why: Memos are spaces for reflection, ideas, quotations, integration, and used to help me build a narrative. One type of memos is research question memos, for example, where I write the content to elaborate the answers to my research question.
Phase 2/Step 4/ Sub-steps a-c. Organize codes into groups with commonalities needed to form themes.	How: “Codes” > “Show Group Code Manager.” (Launch the “Show Group Code Manager” from the “Codes” menu) Why: The grouping of codes by shared characteristics allows me to form themes as part of thematic analysis. Code groups serve as filters. For example, a code group named "Cyber Threat Category" will comprises of codes such as "phishing," "passwords," and "company supplied laptop".
Phase 2/Step 5/ Sub-steps a-e. Create a network to visualize the nodes that are the visualization of the linkages of the themes and units of analysis.	How: “Network” > “Network. Launch Network” from the network drop-down menu. Select codes with similar features and group them.

Phase/Step/Substeps	ATLAS.ti execution details (how and why)
	Why: A network shows relationships between quotations and codes. ATLAS.ti uses networks to help represent and explore conceptual structures. Network displays visualizing linkages. For example, a linkage, code linked to a quotation, shows a connection between elements.
Phase 2/Step 5/ Sub-steps a-e. Analyze data set using tools such as "Word Cruncher" to examine information to find commonalities, differences, patterns, or structures.	How: "Memo" > "New Memo" (Click New memo from the Memo menu). Type the memo. Why: Memos are spaces for reflection, ideas, quotations, integration, and used to help me build a narrative. One type of memos is research question memos, for example, where I write the content to elaborate the answers to my research question.
Phase 3/Step 6/ Sub-steps. Export reports that are output from any of the managers with relevant information.	How: Choose "Output" from any of the Manager menus and select what information is needed in each report. Why: The range of output is from printing the layout to saving a network view to a file. The output may be used as the inclusion of final reports in my doctoral study.

Reliability and Validity

In this multiple-case qualitative study, I incorporated reliability and validity strategies to ensure the quality of the study. Similar to quantitative research, the quality of qualitative research can be assessed in terms of reliability and validity (Leung, 2015). According to Cypress (2017), reliability and validity are essential concepts that should be repetitively operationalized to address the conditions of a qualitative inquiry. This section describes strategies I executed to facilitate reliability and validity in this research paper.

To ensure reliability in this study, I utilized member checking, reflexive journal, and interview protocol. Reliability, in qualitative research, stipulates the consistency and repeatability of the research process among researchers and the study materials (Kihn & Ihantola, 2015). Likewise, Houghton et al. (2013) agreed that reliability is the outcome of an operation that generates a consistent, dependable, and replicable result. Moreover, I used member checking to ensure consistency in my understanding of each participant interview. Furthermore, I used the interview protocol as a roadmap to ensure consistency in the process during interviews. Although the researcher may use different strategies to acquire reliability in qualitative research (Noble & Smith, 2015), it can be arduous to replicate a qualitative study because of the subjective posture of the participants and the researcher. Despite such constraints, the researcher can display reliability by keeping a reflexive journal or a log to chronicle the research process. Therefore, I used member checking, reflexive journal, and interview protocol to show reliability and ensure the research results are dependable and consistent, contingent to the data collection and analysis.

The intents of this qualitative study include accuracy, reliability, validity, and trustworthiness. Kipkulei (2013) pointed out that a researcher's instrument uses is valid, provided it measures what the researcher purposed measuring. Seyal (2015) suggested that two types of validity in research are internal and external. Although internal validity refers to the believability and trustworthiness of the inferences, external validity occurs when the findings of the study can be applied to other contexts such as groups, settings, and populations (Sikorskii & Noble, 2013). Parallelisms exist between four aspects of qualitative and quantitative research where credibility matches internal validity, transferability matches external validity, dependability matches reliability, and confirmability matches objectivity (Morse, 2015). Table 4 displays the similarities of criteria of validity between the qualitative and quantitative research methods.

Table 4

Parallelism Criteria of Validity

Research method	Criterion	Criterion	Criterion	Criterion
Qualitative	Credibility	Transferability	Dependability	Confirmability
Quantitative	Internal Validity	External Validity	Reliability	Objectivity

Member checking and triangulation accomplished credibility, transferability, dependability, and confirmability.

Dependability

In this study, dependability refers to the consistency whereby the results could be reiterated and affect in similar findings. In qualitative research, dependability and credibility are synonymous with reliability and internal validity (Munn et al., 2014). Likewise, I implemented the dependability quality criterion to put in place the reliability of this multiple-case qualitative research. A dependable study allows other researchers to understand and trace the inferences. Houghton et al. (2013) stated that a study reader might disagree with the interpretation of the study; however, they consider the study dependable because the reader can understand how the researcher acquired the study's findings.

I addressed dependability in this study by utilizing member checking. Member checking is one technique researchers use for determining dependability in qualitative research (Welch et al., 2014). The member-checking process involved requesting each participant to review his or her collected interview data for the intended interpretation and accuracy. Houghton et al. (2013) agreed that member checking would ensure the intent and the interpretation of the collected data are the same. According to Beck (2014), the misrepresentation of collected data can affect the validity of the study; hence, member checking was used to counteract such action. After I completed member checking, the surface of new data during the process triggered the repeats of member checking until I acquired data saturation.

Credibility

Credibility refers to the authenticity and trustworthiness of the findings. Member checking assists in the building of a trusting relationship between the researcher and participants (Cheng, 2014). The research study participants are the designated persons to decide whether the results reflect the phenomenon under consideration. Member checking and methodological triangulation were two strategies I employed to achieve credibility in this study. Member checking helped to ensure the collected data are a correct representation of the participant's viewpoint. I utilized multiple research data, such as interview data and hospital documents, to conduct methodological triangulation on the quality of research data during the data analysis to improve the trustworthiness of the study's findings.

Methodological triangulation is a frequently used technique for verifying accuracy that involves double-checking information from multiple sources. Moreover, methodological triangulation is necessary to enhance the validity and rigor of a study (Noble & Smith, 2015). Furthermore, triangulation may provide more robust evidence for the researcher, which improves the credibility of the study (Koc & Boz, 2014). The triangulated data sources for this study were procedure documents, interviews, hospital policies, and standard operating procedures utilized by the hospitals.

Transferability

Transferability, also referred to as external validity, denotes the degree that the findings of the study can transfer to other contexts by the readers. Consequently, the results are generalizable and can be applied to other similar milieus such as settings,

populations, and situations. Allred et al. (2017) defined transferability as the typical comparison of research findings to similar studies to decide possible commonality. Fusch et al. (2018) outlined that in qualitative research, to omit the generalization of the research findings, the understanding of transferability is the onus of the reader and future researcher. I used triangulation and member checking to support data saturation, and I provided descriptions of procedures used for data collection, data analysis, and how I conducted semistructured interviews guided by interview protocol. The researcher should make available an accurate account of the research processes utilized in the study to underpin the concept of transferability and to offer the reader pertinent information to draw an informed determination (Sidhu et al., 2017). I provided readers with evidence of the research study's findings that could be applicable to other contexts, populations, situations, and times. Therefore, I enhanced transferability by making clear the research context and the central findings of the research.

Confirmability

Confirmability is a measure of the objectivity used in evaluating the results and explains how sufficient the research findings are established by the data collected by other researchers. Zachariadis et al. (2013) defined confirmability as the degree to whereby other researchers could confirm or agree with the research findings. Moreover, Erlingsson and Brysiewicz (2017) stipulated that trustworthiness and confirmability can be achieved by accurately describing the methodologies of the flowchart in the study. The strategy I used to accomplish confirmability in this study was the audit trail approach as outlined by Petty et al. (2012). I kept an in-depth audit trail specifying how data were

collected and how categories were derived. I documented the procedures for multiple checking the data during the study. The detailed information allowed an audit trail for other researchers to review the data analysis process, understand my reasoning, and confirm or agree with the findings.

Transition and Summary

In section 2 of this study, I explored the primary purpose of the study, the designated participants, the researcher, the population and sampling, and the methods and processes that were used to gather and analyze the research data. The purpose of this multiple-case qualitative study was to explore the strategies IT security managers use to reduce cybersecurity breaches in hospitals. I used member checking and methodological triangulation to ensure the reliability and validity of this qualitative research. Section 3 of the study comprised the presentation of findings, the implication for social change, a discussion concerning the applicability to professional practice, the recommendations for action and further research, reflections, and the conclusion of the study.

Section 3: Application to Professional Practice and Implications for Change

Overview of Study

In this exploratory multiple case study, I aimed to identify the strategies that hospitals put in place to reduce cybersecurity breaches in hospitals. Previous scholars have conducted thorough research on the implementation of cybersecurity best practices in various organizations to prevent incidents. However, little research has been conducted on strategies for reducing cybersecurity breaches in hospitals.

I incorporated RAT, developed by Cohen and Felson (1979a), as a lens to explore the research participants' understanding of strategies for reducing cybersecurity breaches in hospitals. The content data analysis of the multiple case study comprised an analysis of the data collected from a total population sample of nine cybersecurity IT professional leaders from hospitals in the eastern United States. Data analysis of codes from the coding process and their relationships within the ATLAS.ti qualitative data software resulted in the discovery of 27 subthemes that emerged into seven core themes. The following seven core themes surfaced (emerged) based on methodological triangulation during the data analysis process: (a) ensure adherence to top cybersecurity framework, (b) implement adequate and effective cybersecurity controls, (c) conduct regular cybersecurity risk assessment, (d) maintain an air gap technique backup, (e) cultivate security awareness culture, (f) encrypt all data at rest and in transit, and (g) keep abreast with cybersecurity news and risks.

Presentation of the Findings

The following primary research question underpinned this research: What security strategies do hospital IT security managers use to reduce cybersecurity breaches associated with sensitive data? I addressed the RQ by executing the research data analysis process within the ATLAS.ti qualitative data analysis software, as demonstrated in the data analysis section of this research. Table 5 highlights the ATLAS.ti artifacts spawned from inputs into the software and outputs from the data analysis process. I executed the data analysis process with ATLAS.ti qualitative data analysis software, using primary documents, quotations, and codes to produce core themes that answered the RQ.

Table 5

ATLAS.ti Artifacts

Atlas.ti Artifacts	Input/Output	Count	Study artifacts	Descriptions
Primary documents	Input	41	Table 6	9 interview transcripts data and 32 documents with information from participants
Quotations	Output	436	Table 7	Meaningful interview quotations
Codes	Output	31	Table 8	Representation for quotations
Codes primary document tables	Output	7	Tables 9, 10, 11, 12, 13, 14. 15	Codes' occurrence in 19 primary documents
Network maps of subthemes semantic	Output	12	Figures 2, 3, 4, 5, 6, 7, 8, 10, 12, 13, 15, 16	Groups of related codes
Network maps of core themes	Output	4	Figures 1, 9, 11, 14	Top-level grouping of related subthemes

The research data were input into the ATLAS.ti database, translated into 32 primary documents as shown in Table 6. With strict attention to detail, data analysis of the 32 primary documents and segmenting the data into chunks of informative interview transcriptions resulted in 436 quotations. Table 7 shows a portion of the 436 quotations. Following that, I completed deductive and inductive coding on the research data to represent different quotations from the participants' responses, which resulted in 31 codes. Table 8 shows a subset of the 31 codes from the coding process. The detailed list of the 31 codes is shown in Appendix F.

Table 6

Nineteen Primary Documents for Data Analysis in ATLAS.ti

Primary document	Name
P 1	Case 1
P 2	Case 1
P 3	Case 1
P 4	Case 2
P 5	Case 2
P 6	Case 2
P7	Case 3
P8	Case 3
P9	Case 3
H 1D1	H1:Completed Questionnaire
H 1D2	H1:ReportSecurityIncidentZ
H 1D3	H1:Keeping_Secure
H1D4	H1:Privacy Prog Train Resources
H1D5	H1:Cybersecurity Essential Training
H2D1	H2:Employees breaches of PHI
H2D2	H2:Cyber Incident Response Plan
H2D3	H2:Document_Security_Whitepaper
H2D4	H2:OperationalSecurityGoogle
H2D5	H2: Essential InfoSec Policies
H3D1	H3:O3HitrustRMF
H3D2	H3:Tightening Security After Breach
H3D3	H3:Cyber Basic_Online

Note. P = participant; C = case (hospital); H = hospital; D = document.

The CISO of Hospital-3 shared 20 different documents on their policies. Table 6 shows a list of six of the 20 documents. I have placed a full list of the policies in Appendix G. In this study, I refer to several of the documents by the study name, where H stands for "hospital" and D means "document."

Table 7

Hospital-3 Policies Documents

Study name	Word document: Name of policies
H3D5	CW IS SEC 101 Information Security Management Policy
H3D6	CW IS SEC 102 Endpoint Protection Policy
H3D7	CW IS SEC 103 Portable Media Security Policy
H3D8	CW IS SEC 104 Mobile Device Security Policy
H3D9	CW IS SEC 105 Wireless Security Policy.docx
H3D10	CW IS SEC 106 Configuration Management Policy

Note. H = hospital; D = document.

Table 8

A Subset of the 436 Quotations for Data Analysis of 19 Primary Documents

ID	Name	Primary doc
1:1	And, , explaining to them	P1
1:2	The last question in that	P1
1:3	Like, these are all the	P1
1:4	So, , there are many	P1
1:5	And, you know, this	P1
1:6	You know, and making	P1
1:7	We have our monthly	P1
1:8	So we're looking at	P1
1:9	Are the increased risk,	P1
1:15	we also, , are patching	P1
1:16	, but to do that, you	P1
1:17	And we already	P1
1:18	And then making sure	P1
1:19	They need to be,	P1
1:20	How do we make sure	P1
1:21	I would say this is acted	P1
1:22	And, uh, this is the	P1
1:23	So essentially how	P1

Table 9

A Subset of the 31 Codes From Deductive and Inductive Coding

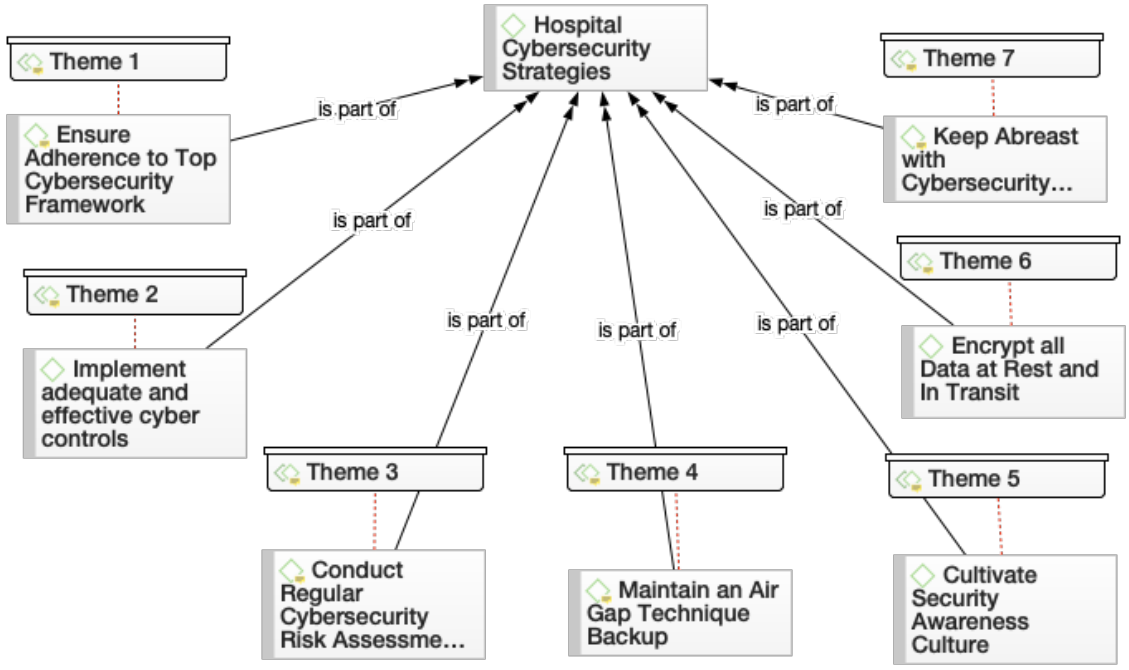
Codes
Build a robust cybersecurity policies and procedures
Check vulnerability and risk advisory feeds
Conduct regular cybersecurity risk assessments
Continue security education training and awareness (SETA)
Create an incident response plan
Cultivate security awareness culture
Do system update/patching
Encrypt all data at rest and in transit
Ensure adherence to HIPAA rules at every stage
Ensure adherence to top cybersecurity framework
Ensure data backup
Ensure strong password
Establish a cyber risk management committee
Follow security influencers and professionals
Hospital cybersecurity strategies

I determined data saturation by applying the data analysis methodology on ATLAS.ti data from eight research participants, which resulted in discovering the 19 codes. Further analysis of the research data from the final participant unearthed no additional codes, leading to the foregone conclusion that I had reached data saturation. However, the reported results included codes from the nine participants' responses, although eight would have satisfied the requirement. The following step was creating ATLAS.ti semantic network maps by scrutinizing the relationships between the 19 codes, which proliferated to tree structures called the study's core themes.

Seven core themes were generated based on methodological triangulation during the data analysis process. The following themes unfolded: (a) ensure adherence to top cybersecurity framework, (b) implement adequate and effective cybersecurity controls (c) conduct regular cybersecurity risk assessment, (d) maintain an air gap technique backup, (e) cultivate security awareness culture, (f) encrypt all data at rest and in transit, and (g) keep abreast with cybersecurity news and risks. To determine each of the core themes, I formulated a well-defined network diagram within ATLAS.ti by mapping pertinent interview quotations to primary codes (nodes) and arcs corresponding to nodes in an upward or inverted rooted tree which formulated the top-level node representing the underpinning or core theme. All seven of the core themes aligned to the RAT conceptual framework. The next step was the presentation of the detailed analysis by core theme. Figure 1 shows an ATLAS.ti semantic network representation of all the core themes.

Figure 1

Core Themes



Core Theme 1: Ensure Adherence to Top Cybersecurity Framework

Cybersecurity framework adherence emerged as the first core theme and an essential strategy from the research data to reduce cybersecurity breaches in hospitals. This core theme aligned with the second of the three notable features of RAT: a suitable target or victim. Figure 2 shows an ATLAS.ti semantic network representation of the build robust cybersecurity policies and procedures subtheme (code), which is a subset of ensure adherence to top cybersecurity framework core theme (code) 1, which is a part of the cybersecurity of hospital, the project of the study. Hence, this is a hierarchy diagram.

Within the RAT construct, the authors (Cohen & Felson, 1979a) argued that a crime happens when three criteria are present: (a) a motivated offender, (b) a suitable

target, and (c) the absence of a capable guardian. The theory constitutes the understanding that crime is ordinary and is contingent on available opportunities. Because the hospital's IT infrastructure, a suitable target, does not have directives from the cybersecurity framework to be implemented, the RAT framework aligns with Core Theme 1. Moreover, the lucrative reward of PII and PHI enhanced the commitment to a crime. Therefore, crime does not require a hardened criminal, convicted felon, or super-predator. Subsequently, all that needs to be present for an offense to happen is an opportunity. RAT theory is pertinent to Core Theme 1 because it provides a clear understanding of why individuals engage in cybercrime. Thus, Core Theme 1 ensures adherence to a top cybersecurity framework and erases the opportunity for a crime by eliminating the suitable target and providing directives for the protection of the IT environment. Cybercrime relates more to the effectiveness of indirect guardianship.

Table 9 shows all nine participants contributed to the discussion of build robust cybersecurity policies and procedure subtheme. In the analysis, I used 16 documents. Hospital-3 CISO provided twenty sterilized documents, from H3D5 to H3D24 (see Appendix G), with detailed information on cybersecurity policies. The IT security managers of Hospital-3 in H3D5 stipulated that the policy applies to all Hospital-3 workforce members and all Information Technology (IT) assets. P7 of Hospital-3 articulated that they are not allowed to discipline anybody if the violation is not in the policies. The core theme formed an integral part of the literature review.

Figure 2

Subtheme: Build Robust Cybersecurity Policies and Procedures

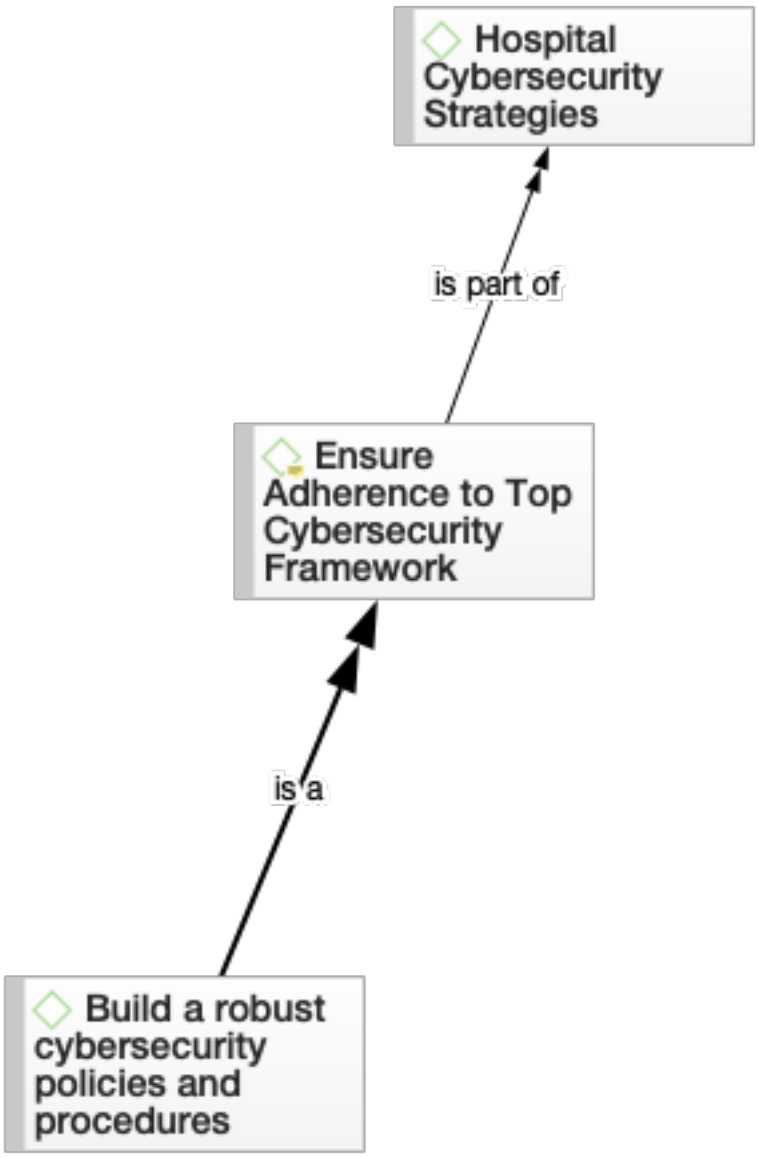


Table 10

Frequency of Participants (Max n = 9) Using Subthemes for Ensure Adherence to Top Cybersecurity Framework

Subtheme	*n*	% of the frequency of participants
Build robust cybersecurity policies and procedures	9	100%
Documents	27	84%

Note. *n* = frequency of participants.

Subtheme 1.1: Build Robust Cybersecurity Policies and Procedures

One hundred percent of the participants strongly endorsed enforcing cybersecurity policies and procedures in their hospitals. The documents (H1D5 and H2D5) from the first two hospitals and P1, P2, P4, and P5 corroborated the cybersecurity framework National Institute of Standard and Technology (NIST) 800-53 as a guide for the formulation of their cyber policies and procedures. While Hospital-3 (P7, P8, P9) is using HITRUST (H3D4) CSF (Common Security Framework) which is robustly based on International Organization for Standardization (ISO) and International ElectroTechnical Commission (IEC) 27001 (ISO/IEC 27001). All three participants (P7, P8, and P9) confirmed that the cybersecurity policies and procedures are based on HITRUST framework, which is generated from the ISO/IEC 27001. HITRUST structured the CSF on ISO/IEC 27001 (H3D1). Two top CSF, NIST 800-53 and ISO/IEC 27001, are risk-based approaches to managing risks in organizations confronted with cybersecurity viewpoints (Ibrahim et al., 2018). All the participants (P1 to P9) accepted that their IT

departments should implement cybersecurity policies and procedures (H1D5, H2D3, & H3D1).

Against the backdrop of cybersecurity strategies in place to minimize breaches in hospitals, the IT infrastructure requires starting with solid cyber policies and procedures. In H1D3, I found the statement which stated that they implemented security controls in their local environment consistent with Hospital-1 policy and standards. Subsequently, P3 of Hospital-1 suggested everything flows down from cyber policies and procedures, such as all the information security controls built from their robust premises. Moreover, P3 emphasized that the hospital's C-exec leadership should accept the responsibility to sign off on excellent cyber policies and procedures because running the IT security process depends on implementing specific regulations or best practices. However, the foundation of cybersecurity policies and procedures is the adaptation of cyber frameworks, such as NIST 800-53, ISO/IEC 27001or HITRUST (P1, P4, P8, P9), which must match the hospital's IT environment. Thaduri et al. (2019) advocated that cybersecurity frameworks are effective solutions for implementing controls, for example, to understand the threats against network endpoints (medical devices), detect the vulnerabilities, accept or reject the risks, and provide the recovery. However, they are usually generic, necessitating customization to be employed in the organization's environment. The hospital-wide information security management program (ISMP) will address all applicable, scoped HITRUST controls, and other hospital specified controls in policies, standards, and processes (H3D5). Moreover, P8 revealed that with a framework like HITRUST, they have a dedicated set of guidelines that they implement through policies and processes that

become their incident response program. Therefore, IT policy and procedure makers must extract relevant recommendations from the general contents of the cyber framework to fit their IT infrastructure.

P7 and P9 of Hospital-3 stipulated that well-adapted cybersecurity policies and procedures set the standards of behavior for activities such as encryption of email attachments and restrictions on the use of social media. Moreover, P7 insisted that if such cyber policies and procedures are not in place, the authority to discipline employees who violate policies will be lacking. Chowdhury et al. (2020) purported that those employees, who are under time pressure, are likely to perform nonsecure workaround without regard for the potential consequences of their actions. Furthermore, employees view information security as an additional but unnecessary burden because the infosec leaders do not integrate policies and procedures in the regular operation of the hospital's IT environment. In H2D5, I extracted that documenting cyber security policies and procedures is time-consuming, but the process is efficient by using a template for NIST-800-53. P4 stipulated that the IT security professional implemented policies and procedures which may make it harder for the employees to access their equipment and find it difficult or time-consuming to perform a specific job function.

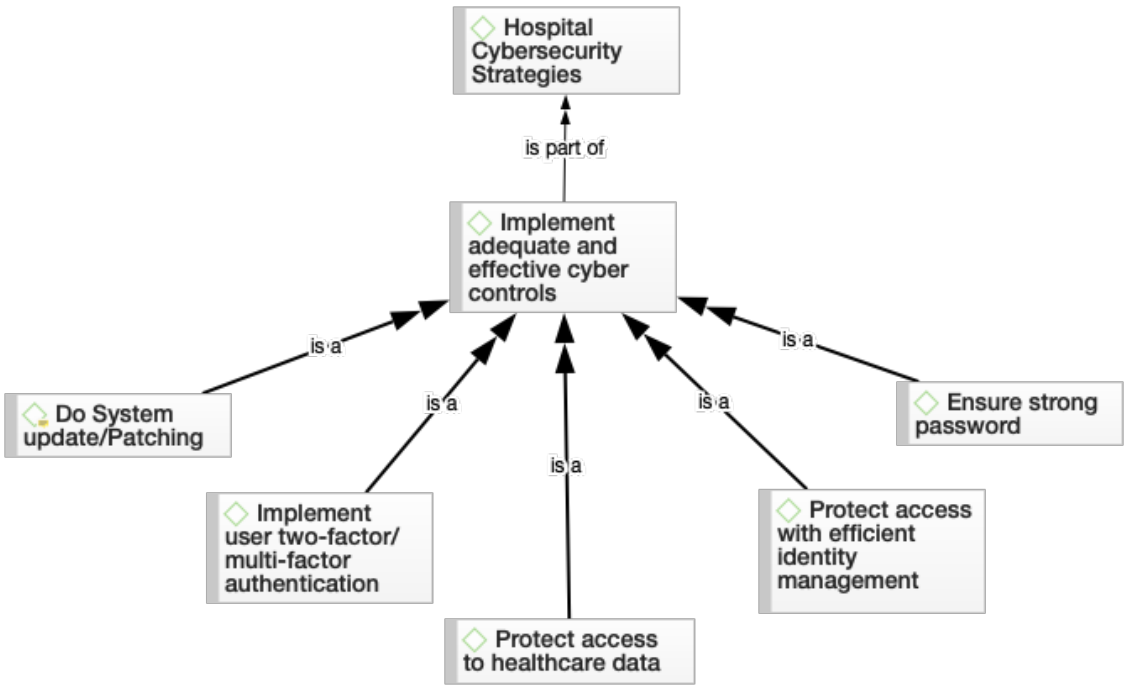
Core Theme 2: Implement Adequate and Effective Cyber Controls

The second core theme that emerged from the research data was implementing adequate and effective cyber controls to reduce hospitals' cyber threats. The core theme aligned with the third criterion of RAT conceptional theory: the absence of a capable guardian (see Cohen & Felson, 1979a). The lack of these cyber controls will contribute to

cyber-attacks creating the opportunity for cybersecurity breaches. In criminology, RAT is categorized as an opportunity viewpoint which maintains that the root cause of criminal events is criminal opportunities (Reyns, 2015). Its central teaching elucidates those crimes happen when the opportunity presents itself due to the convergence of the three criteria. Hence, to apply RAT in this situation, the hackers will act upon the network, which presents the unprotected IT infrastructure because no cyber controls are implemented. This second core theme is ubiquitous throughout the literature review. Figure 3 shows an ATLAS.ti semantic network representation of the emergence of the second core.

Figure 3

Core Theme 2: Implement Adequate and Effective Cyber Control



As shown in Figure 3, five emergent subthemes evolved from the data analysis into the core theme. I generated the results shown in Table 10 by analyzing the Code Primary Document Table from ATLAS.ti for Core Theme 2. Table 10 shows different percentages of participants based on the subtheme shared information that generated codes used in mapping the strategies for reducing cybersecurity breaches in hospitals.

Organizations, including hospitals, presently understand that they should be examining and follow their security controls through normal best practices such as patching reports, risk assessment, vulnerability assessment, audit, internal audit, information risk assessment, cyber risk assessment, internal audit, penetration testing, audit, and antivirus software updates (Evans et al., 2016). Cybersecurity controls are processes used to detect, prevent, and mitigate cyberattacks and threats (H1D3, H2D3 & H3D10). Thus, cybersecurity controls are mechanisms used to prevent, detect, and mitigate cyber threats and attacks. Mechanisms cover a gamut of controls such as physical controls, including security guards and surveillance cameras, to technical controls, including but not limited to firewalls and multifactor authentication.

Table 11

Frequency of Participants (Max n = 9) Using Subthemes to Implement Adequate and Effective Cyber Controls Core Theme

Subtheme	*n*	% of the frequency of participants
Do system update/patching	9	100%
Implement user two-factor/multifactor authentication	3	33%
Protect access to healthcare data	9	78%
Protect access with efficient identity management	9	100%
Ensure strong password	3	33%
Documents	16	50%

Note. *n* = frequency of participants.

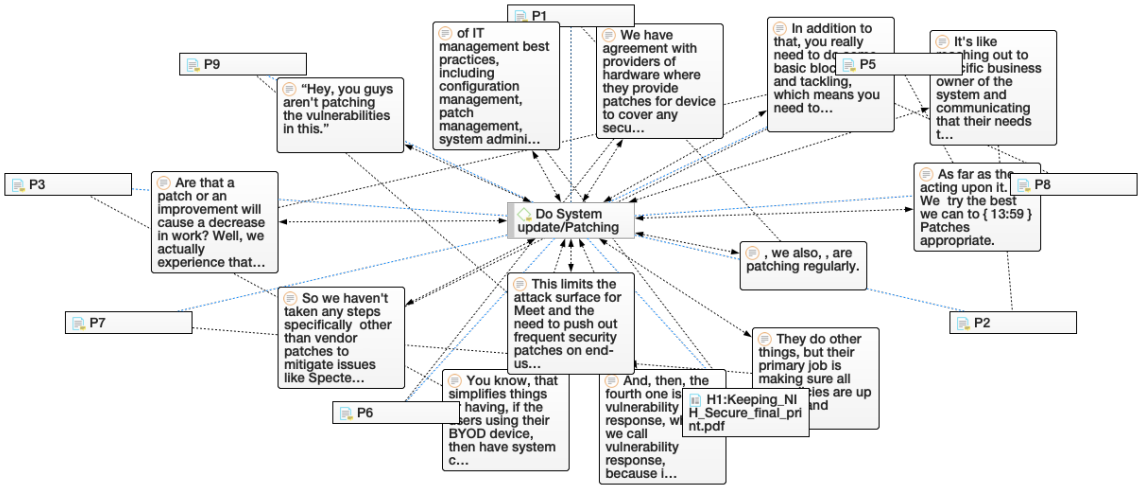
Subtheme 2.1: Do System Update/Patching

All research participants (100%) acknowledged regular patching and updating of software. Figure 4 shows an ATLAS.ti semantic network representation of the emergence of this subtheme. P1 categorically stated that they conduct patching regularly. Hospitals' IT environments have software patching practically every day, which makes it extremely difficult to comply with Food and Drug Administration (FDA), a regulatory authority, a recommendation as to how to manage cybersecurity risks to keep safe the patients and the information housed, protected and processed by the medical device (Williams & Woodward, 2015). P5 shared an incident that required patching, and afterward affected performance. P5 stated that in the emergency room (ER), they were compelled to patch a

device used for e-prescribing; subsequently, the instrument increased in performance. All three hospitals shared documents with patch management, the mechanism for issuing and applying software updates to correct vulnerabilities (H1D1, H1D3, H2D3 & H3D2). Most participants (P2, P3, P4, P5, P8, and P9) echoed that their hospitals are uniquely challenged beyond standard patch management barriers. However, they continue to keep in compliance with software patching and updating.

Figure 4

Subtheme: Do System Update/Patching

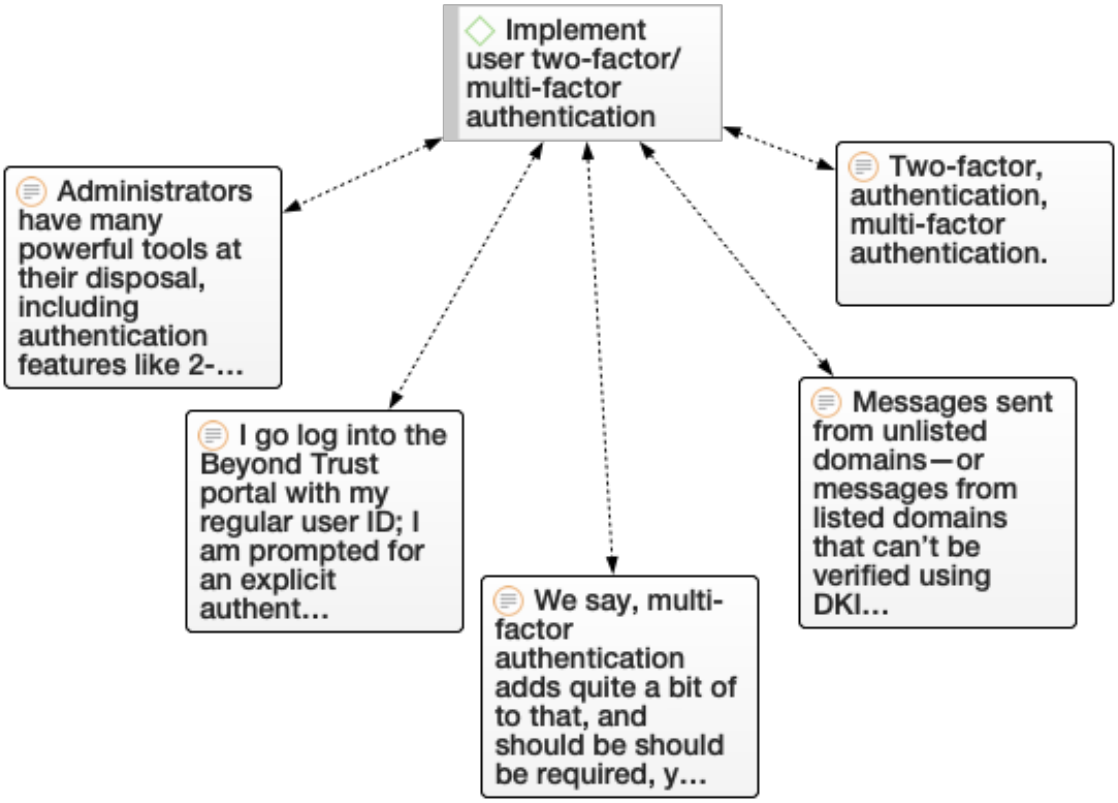


Subtheme 2.2: Implement User Two-Factor/Multifactor Authentication

Thirty-three percent of the participants shared responses on implementing user two-factor or multifactor authentication as one of the subthemes of Theme 2. Figure 5 shows a network map of the implemented user two-factor or multifactor authentication subtheme that contains codes and participant quotations (P3, P6, and P9).

Figure 5

Subtheme 2.2: Implement User Two/Multifactor Authentication.



The Health Insurance Portability and Accountability Act (HIPPA) requires covered entities to ensure that anyone requesting access to electronically protected health information (ePHI) is authorized (Blanke & McGrady, 2016). Multifactor authentication (MFA) offers hospitals this type of secure access and adequate security to keep vector attackers away. With regular user credentials, P9 logged in to Beyond Trust, a software that supports privileged identity management and access management, where they are prompted for an explicit multifactor authentication to access resources. Subsequently, the authentication mechanism should be designed to accomplish the pinnacle security level

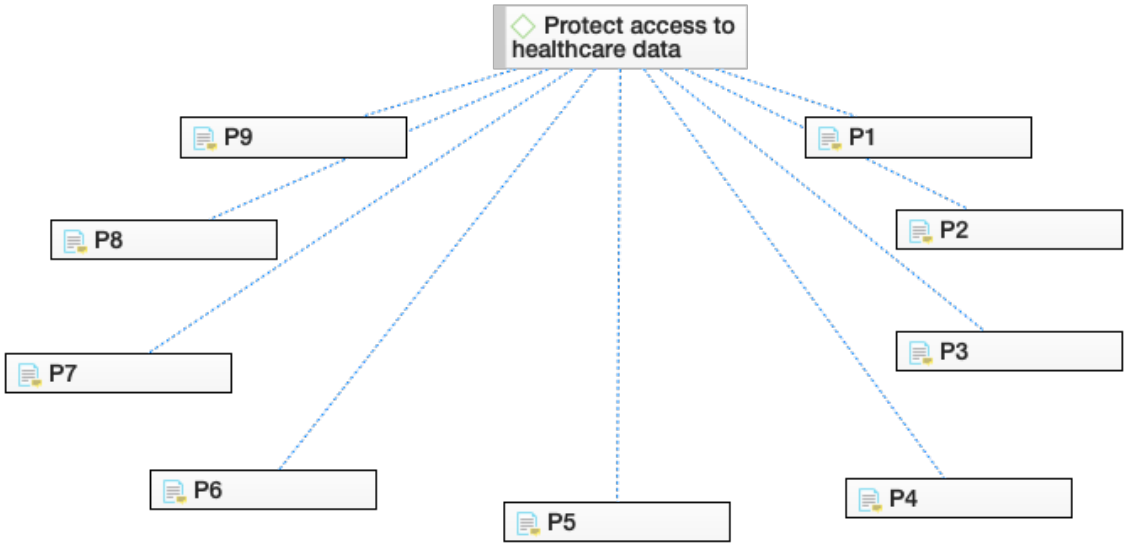
using a mutual multifactor authentication scheme. This process reduces illegal access to ePHI (Yaacoub et al., 2021). In H2D3, I found the directive that Hospital-2 implemented multifactor access control with security badges and biometrics. According to P3, multifactor authentication provides a well-needed cybersecurity strategy requiring the user's account wanting to access sensitive data.

Subtheme 2.3: Protect Access to Healthcare Data

An overwhelming subtheme from this study is protect access to healthcare data which all participants (100%) contributed to the conversation. This subtheme aligned with the RAT conceptual framework as it relates to the three main criteria (a motivated offender, a suitable target, and the absence of a capable guardian). It permeated the literature review. Figure 6 shows a network map of protect access to healthcare data subtheme containing participants who supported it.

Figure 6

Subtheme 2.3: Protect Access to Healthcare Data.



A representative from all three hospitals (P1, P4, P6, P7) concurred that they are responsible for healthcare data security. P6 stated that they are responsible for the security landscape of the organization, such as the security practices, the OKR (objectives and key results), the protection of the healthcare data, the protecting of access to essential data, and making sure that whatever products or services that the hospital would like to implement is done. When hospital employees are empowered to decide to protect the healthcare data, it could improve the hospital's security posture (H2D3). Swede et al. (2019) concluded that the protection of patient data emerged as an integral part of the responsibility of entire healthcare professionals. They further stipulated that regular data breaches highlight the significance of training healthcare stakeholders, including clinical employees, in protecting healthcare data. (Swede et al., 2019). Consequently, all hospital stakeholders consider that protecting healthcare data are of utmost importance.

P3 warned of system anomalies where they will detect significant things of concern, such as exfiltration of data, in which case abnormalities of the volume of data are being sent to an unwanted destination. Healthcare data breaches are increasing exponentially yearly and will continue to accelerate weekly (Pigni et al., 2018). Therefore, it is essential for healthcare IT professionals to protect their IT infrastructure from both external threats such as hackers and cyber criminals or internal threats such as access abuse leading to loss of data (Pigni et al., 2018). Healthcare data security is a significant component of HIPAA rules (H2D1, H3D1 & H3D2). Regarding the hackers' method of implementing ransomware, P7 explained that the hackers would encrypt the hospital backup first. They will exfiltrate much of the healthcare data, followed by them encrypting the healthcare data. Although data loss protection (DLP) tools ensure that sensitive data are not accessed, misused, or lost by unauthorized users, their primary purpose is not to discover vulnerabilities but to prevent data loss and to detect and protect healthcare data (P2). The IT personnel encouraged the workforce that if they know or suspect that the compromised device has sensitive data, they are to follow specific steps for mitigation (H1D2). Moreover, IT security engineers used the Google workspace tool to prevent exfiltration, which is data improperly removed or sent outside of the hospital system (P6). Therefore, healthcare data are valuable on the black market since it often includes an individual's PII. At the same time, hackers may find a single piece of information such as social security number, password, or mother's maiden name in a financial breach.

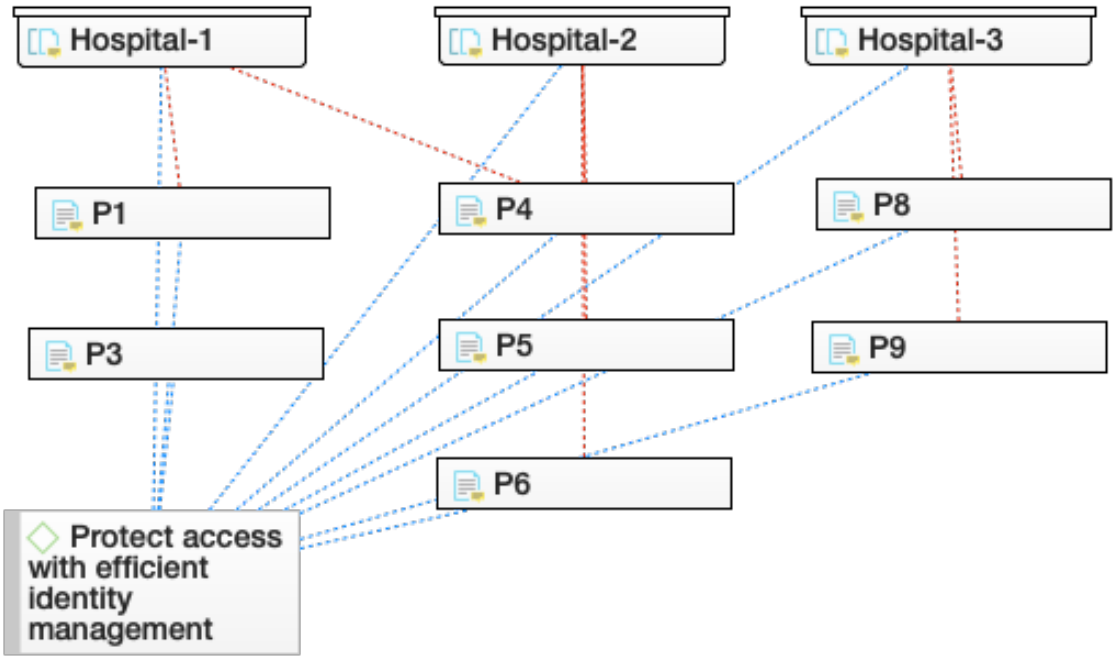
P3, P6, P8, and P9 agreed that securing their network perimeter and improving perimeter defenses should be top priorities for any hospital that values cybersecurity. P6 and P8 recommended that hospitals build a firewall as the first line of defense because it builds a virtual wall around their network and IT infrastructure. A firewall is a network gateway (security guard) placed at the point of entry between an organization's on-prem network and the outside Internet, where all incoming and outgoing packets traverse (Khoumsi et al., 2018). Apart from a firewall, other controls such as intrusion detection systems (IDS), intrusion protection systems (IPS), virus protection, malware protection software, sandboxing technology for email phishing protection, endpoint detection and response (EDR) technology, and more cybersecurity perimeter (P2, P3, P6, P8, P9) must be implemented. The contents of H1D5, H2D3, H3D1, and H3D2 contain multiple mechanisms for the protection of sensitive healthcare data. Over time, the methods used for cybersecurity perimeter have improved to better secure hospital real-time applications and provide adequate healthcare data protection.

Subtheme 2.4: Protect Access With Efficient Identity Management

Seventy-eight percent of the participants pointed out within the research that data protection access with efficient identity management is a strategy for reducing breaches in hospitals. Figure 7 shows a network map of protect access with an efficient identity management subtheme that contains codes and hospitals with participants (P1, P3, P4, P5, P6, P8, and P9).

Figure 7

Subtheme: Protect Access With Efficient Identity Management



The protect access with efficient identity management subtheme aligned with all three criteria of the RAT conceptual framework and is prevalent through the literature review. Identity management (IdM) is also defined as identity and access management (IAM) in the documents. Generally, IdM denotes a constraint of technologies and policies for verifying that only authorized end-users can access the related resources in an organization (Liu et al., 2020). P4 explained that the IT professional implemented identity policies, which appeared to make the process harder to access the equipment. They are more complex or time-consuming in performing a specific job function and accessing resources. Information Technology (IT) requires that identified mobile devices connect to the hospital network or store and access the hospital's sensitive information,

maintain secure configurations, allow for monitoring and software updates, and, if necessary, remove healthcare-sensitive data and applications (H3D8). P3 suggested that it is common practice that the IT tools used for identity management are not only looking at the user but also the original location of the user's device. According to one of the documents provided by P1 at Hospital 1, a report by the Identity Theft Resource Center, data breaches are up 38% in the second quarter of 2021, with signs trending towards an all-time high for this year. Subsequently, P9 pointed out that hackers, whom we must identify, are not authorized users or employees, and they seek to steal information for identity theft or some other financial crime.

Subtheme 2.5: Ensure Strong Password

Thirty-three percent of the participants (P3, P8, P9) acknowledged using a strong password as the fifth subtheme. The IT department ensures that everyone follows the hospital's password policy which should be long, complex, and easy to remember password (H1D4 & H3D14). P3 stipulated that strong password control will determine what is accessible and within what window of time access is allowed for Hospital-1. I obtained information from Hospital-1, which stated that hacked passwords are top of the list of root causes of data breaches, and it comes as no surprise considering individuals set weak passwords such as "123456" and "Password." Following their studies, multiple researchers recommended that users make solid, easy-to-remember passwords. To ensure IT infrastructure protection, users should follow the password defense guidelines (Khalind, 2019). Stobert and Biddle (2018) stated that while users create, remember, and keep up with many passwords, they find managing passwords arduous. P8 noted that

configuring devices, which are not easily breached, involved having complex passwords, and they denied everyone from the devices.

Core Theme 3: Conduct Regular Cybersecurity Risk Assessment

The following core theme from the study data analysis is conduct regular cybersecurity risk assessment. This theme is related to the preventative aspect of the RAT conceptual framework. While it is challenging to deter the happening of motivated offenders (cybercriminals), suitable targets (hospital IT infrastructure with lack of cyber risk assessment) in cyberspace and virtual guardianship may drive crazy motivated offenders and reduce the impact of cyber compromises. Although some contentions about applying the RAT to cybercrime, RAT undoubtedly contributes a significant role in comprehending the real cause of criminalization and victimization in cyberspace. Moreover, this theme is pervasive throughout the literature review. According to Coronado and Wong (2014), cybersecurity risk management is of tremendous responsibility, which requires all the stakeholders in the healthcare community to continue to be cognizant of the process as they protect their services to ensure the highest delivery of patient care. According to various standards and industry methodologies, information security risk assessments (ISRA) are performed daily (Shameli-Sendi et al., 2016). In response to the frequency of cybersecurity risk assessment, P1 replied that we conduct simulations, a cyber risk assessment component, every couple of months. While P2 disclosed that they conduct regular risk acceptance on their legacy system to assess the threats, vulnerabilities, and impacts on the hospital IT infrastructure. Argaw et al. (2020) purported that cybersecurity risk assessment is contingent on knowing the at-risk

IT assets emphasized by the NIST cybersecurity framework (CSF) for a real-time IT environment and filtering out the threats through processes such as vulnerability management. The cyber risk assessment is documented in the risk register and used to inform executive management of the risk and the options for managing risk (H3D21). P7 outlined that the security operations team constantly modifies their environment in response to the inputs from the threat intelligence feeds. Moreover, P7 explained that they got a group of IT professionals, about five individuals, who are dedicated to threat management and to look for new threats, and they make sure they adjust their posture to match the threats. Furthermore, P7 continued and said they work closely with the security operation team and run many tabletop exercises yearly. Thus, the running of frequent cyber risk assessments benefits the hospital by revealing the potential threats and vulnerabilities, allowing the InfoSec team to mitigate any breaches.

A practical cybersecurity risk assessment involves identifying threat sources, events, and vulnerabilities. Moreover, it decides the likelihood of exploitation and probable impact on the hospital's IT environment while calculating the risk as it integrates likelihood and effect. Offner et al. (2020) outlined that a cyber risk assessment names the different information assets that are potentially affected by a cybersecurity attack affecting IT systems, desktops, hardware devices, tablets, laptops, intellectual property, and healthcare data, followed by categorizing the risks that probably affect such assets. A cyber risk assessment could assist the workforce on expected threats to confront the hospital, the location of the threats, and how the threats will affect their function (H1D1, H2D3, & H3D21). Jouini and Rabai (2016) concurred when they stated that

cyber risk assessment is necessary in the information security management framework because the hospitals adopt a step-by-step and well-structured mechanism for calculating cybersecurity risks to their assets. P3 explained that the hospital might have policies and procedures. However, to ensure that those policies and procedures are implemented, the audit division or source must test those cyber risks to ensure that they are enforced from the lowest level upwards. P6 suggested that the IT personnel deal with massive risks such as PHI and PII after cyber risk assessment. P8 expounded that the assessment tool, Aramis, allows them to know what risks they have, what security their posture is, and then be able to make appropriate decisions as to whether it is a threat. It can update and change the configuration of a hospital device. Using ATLAS.ti, table 11 shows the frequency of participants regarding subthemes for conduct regular cyber risk assessment core theme. Nine participants (100%) subtheme identified cybersecurity risks contributed, while seven participants (78%) shared information on the subtheme plan for incident management. In the analysis, I used 12 documents (37%).

Table 12

Frequency of Participants (Max n = 9) Using Subthemes for Conduct Regular Cybersecurity Risk Assessment Core Theme

Subtheme	*n*	% of the frequency of participants
Identify cybersecurity risks	9	100%
Plan for incident management	7	78%
Documents	12	37%

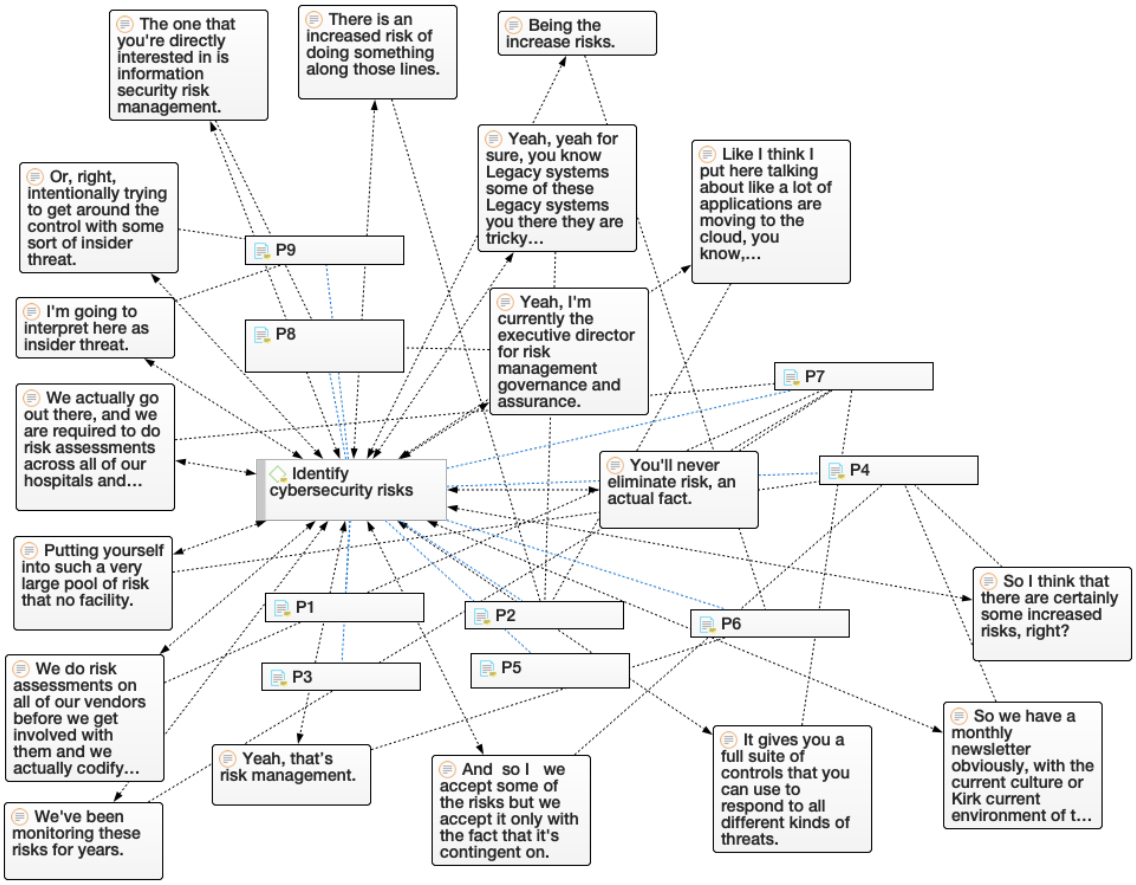
Note. *n* = frequency of participants.

Subtheme 3.1 Identify Cybersecurity Risks

All research participants (100%) pointed out that identifying cybersecurity risks contributes to reducing cybersecurity breaches in hospitals. Figure 8 shows a map of multiple input data sources subtheme containing codes and participant quotations.

Figure 8

Subtheme: Identify Cybersecurity Risks



Cybersecurity risk identification may be a little complicated because the field of cybersecurity is evolving. Hence, cybersecurity risks are difficult to define clearly. The acceptable basic approach used to identify cybersecurity risks involves: (a) identifying your assets, (b) identifying the threats to those assets, and (c) identifying the

vulnerabilities to those threats (Esteves et al., 2017). P7 stated that if the Infosec leaders do not have a complete and accurate inventory of everything on the network, they cannot protect them. The HITRUST document (H3D1) contains the risk assessment process, which identifies the ability to create capital and operational project plans for defined security services according to vulnerabilities for specific cyber control. The first step to identifying cyber risk is covered by having an accurate inventory of the assets in the IT infrastructure. P9 emphasized that they know how many medical devices (assets) they have, where the devices are, and their risk posture is versus their baselines. P1 mentioned that they do a risk assessment of the environment to ensure that they know and prioritize their assets to make a big difference as a whole. P6 pointed out that medical equipment, the primary asset in the hospital environment, is higher for attacks. Having identified the hospitals' assets, such as medical equipment (medical devices), patients, and other stakeholders' data (PHI, PII), I will identify the threat to the identified assets.

Cyber threat analysis entails pinpointing likely sources of abuse to the assets (data, information) the hospital is responsible for protecting. With the joining of medical devices with healthcare data, external and internal cyber threats are continuing to increase. Hence to reduce such assets' threats, relevant devices must be tagged and prioritized (Kim et al., 2020). Seventy-eight percent of the participants (P1, P4, P5, P6, P7, P8, and P9) have cybersecurity tools to identify cyber threats. For example, P1 elucidated that their cyber tool provides them with a malware checklist which activates a first step process is a particular threat. Moreover, P8 outlined that they rely on a best practices vendor to aggregate where those security issues are. Then they use that

technology to scan their environment to ensure that they are keeping their environment up to date and they are protected from those newly emerging threats. The effort of the IT c-executive to invest in strengthening critical security infrastructural and information privacy could remove the blind spots for identifying risks, protecting the endpoints on the hospital network, and performing cyber risks assessment that could protect critical and sensitive data (H1D3). Furthermore, P7 emphasized that when they get a threat advisory, which details the techniques, tactics, and procedures that these hackers are using, which could be the signatures of malware. They welcome this kind of threat feed because they are alerted to activate the defense security. They gleaned from a document I received from Hospital-1, which noted that understanding how these threats and failures occur is critical in determining the best way to limit points of vulnerability.

After known threats, the following process is to identify vulnerabilities (weaknesses) in the entire cyber environment that could expose the IT infrastructure to those threats. Williams and Woodward (2015) categorized cyber vulnerability as a weakness likely to be manipulated, whether it is in operating systems, networks, hardware, software, medical devices, firmware, processes, and people. All these entities include an information system and are mission-critical to their operation. One of the most urgent tasks of Infosec professionals in detecting cyber vulnerabilities in hospitals, which may violate the basic triangle of cybersecurity, namely confidentiality, Integrity, and Availability (CIA). For example, they were stealing confidential healthcare data, breaking data integrity, or denying system availability. The hospital's security technicians and subject matter experts support risk management obligations (H3D3). P7 denoted that

their vulnerability management requires that all critical vulnerabilities be remediated within 30 days of being identified; high vulnerabilities remediated within 60 days; medium vulnerabilities remediated within 90 days; and low vulnerabilities remediated within 120 days. P5 acknowledged that they have a very robust vulnerability management program, ensuring that all their findings, such as missing patches or configuration vulnerabilities, are remediated quickly. P2 declared that their hospital's IT and Infosec infrastructure have vulnerability scanning agents that will scan daily. In some cases, they scan across all their components every week, which would identify any vulnerabilities that emerge.

Subtheme 3.2: Plan for Incident Management

Seventy-eight percent of the research participant provided information on the second subtheme: Plan for incident management. They stressed the importance of having an incident management plan to ensure business resumption in the fastest and safest way possible. A cyber incident management plan (IMP, H3D19), also known as an incident response plan, business resumption plan, or emergency management plan, is a document that outlines a hospital's resume to normal as rapidly as possible after an unplanned cybersecurity event (Naseer et al., 2021). A cyber incident management plan is a document of guidelines that direct IT Infosec teams on how to prepare for, detect, respond to, and recover following a cyberattack incident. P8 suggested that with a framework like HITRUST, they have a dedicated set of guidelines that they implement through policy and process that become their incident response program. Hospital-3 IT leadership developed and implemented an IMP that effectively reports, responds to, and

documents security incidents that could likely compromise the CIA-triad of their IT assets (H3D19). P1 explained that if there is a suspected incident, they would be prepared because they have a plan involving an enterprise tool that records these incidents and remediates the issue on time. The increasing trend in ICT (Information and Communication Technology) disruption of normal operations makes cybersecurity and digital continuity a problem that should address in hospital disaster preparedness (Klokman et al., 2021). P4 stated that they had covered the cybersecurity framework to investigate and remediate an incident because the question is not if they are going to have an incident but when are they going to have an incident, so they must be prepared just in case it happens.

Core Theme 4: Maintain an Air Gap Technique Backup

Maintain an air gap technique backup for a strategy to reduce cybersecurity breaches in hospitals emerged from the study data. This core theme is congruent with the RAT conceptual framework; the third criterion is the absence of a guardian or custodian of data. In a study, the researchers tried to have some clarity on the difficulties of malicious threats to cyber breaches and digital forensics by using the RAT, which consists of three main criteria: (a) motivation, (b) opportunities, and (c) guardianship (Ab Rahman et al., 2017). In the event of a ransomware attack, if the victim, which is the hospital's IT infrastructure, does not have an available backup, then the final guardianship is not public to recover the IT environment. Hence, the backup of the hospital data protects the IT environment from disaster through the ultimate last resort to restore from backup.

This core theme reflects one of the main contents of the literature review. Argaw et al. (2020) recommended that the information security team should utilize the maintenance of regularly updated backup (which should be stored offline) as a crucial tactic for reducing exposure to cybercriminals. Moreover, Chandna and Tiwari (2021) purported that the most common cyber and risk management best practices have a reliable and resilient backup system to provide the business with offline backups, allowing the hospital to function normally. Hospital-2 document (H2D2) addressed the question of what to do when a cybersecurity breach occurs, and the answer was to identify your external resources and backup. P4 stated that their hospital essentially implemented offline backups, also known as air-gapped backup. They continued that such storage is disconnected from the Internet and are isolated copies of the healthcare data that cannot be accessed through the network. P7 acknowledged that they have air gap backups because the cyber attackers who use ransomware attacks will, typically, encrypt the potential victim's backups first. They exfiltrate much of the hospital's data. Next, they encrypt the hospital's data. So, if the hospital tries to recover from the loss of healthcare data, they will suddenly find out that the backup is unavailable because the cyber attacker encrypted the backup. However, an air-gapped backup does allow the hospital to isolate their backup for recovery from ransomware or other cybersecurity breaches. I generated the results shown in Table 12 by analyzing the Code Primary Document Table from ATLAS.ti for core theme 4.

Table 13

Frequency of Participants (Max n = 9) Using Subthemes for Maintain an Air Gap Technique Backup Core Theme

Subtheme	*n*	% of the frequency of participants
Ensure data backup	6	67%
Documents	7	22%

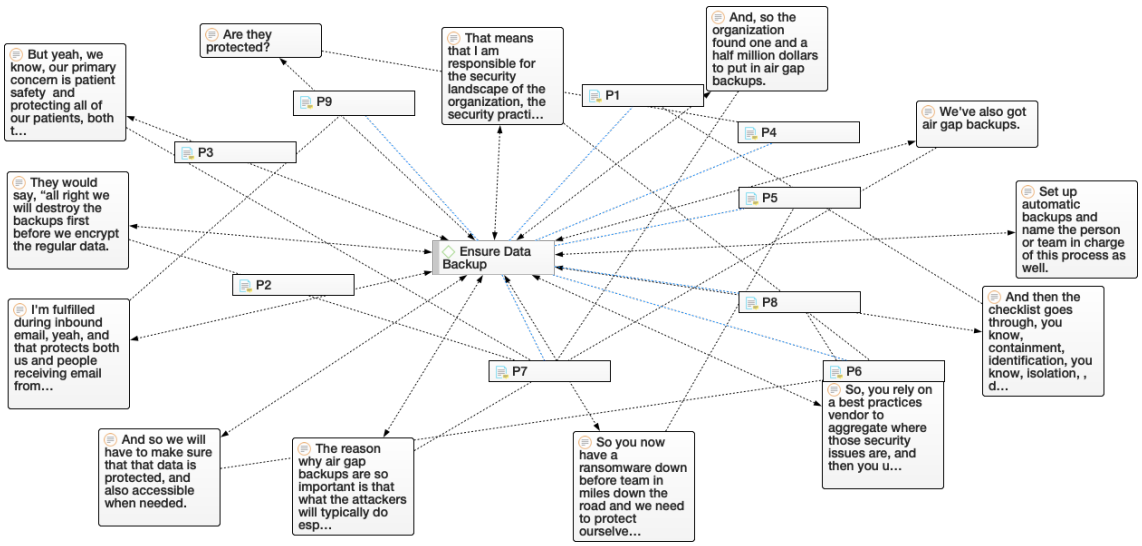
Note. *n* = frequency of participants.

Subtheme 4.1: Ensure Data Backup

Sixty-seven percent of participants accepted that to ensure data backup is completed daily. In the analysis, I used 7 documents (22%). Figure 9 shows a network map of the ensure data backup subtheme that contains codes and quotations from participants.

Figure 9

Subtheme: Ensure Data Backup



P8 emphasized that there are three tasks to remember for cybersecurity in the hospital: backup, backup, and backup. The best countermeasure for ransomware is always having a recovery backup available (P2, P5, and P7). P7 outlined that the hospital's ability to restore data that adhere to the security triad (CIA) when requested promptly is one of the most significant data protections against cybersecurity breaches such as hacking and ransomware. Although the hospital experienced an incident of hacking that demanded payment in return for unencrypting the patients' record database, the hospital reported that its backup system possessed an up-to-date and less than a half-day of data lost (Argaw et al., 2020). The above scenario demonstrated the significance of having an updated backup of the hospital data. Subsequently, restoring lost data after a successful cyberattack requires the most recent unaffected backup (air-gapped backup), which can be used to restore lost data because the backup data were on offline devices or systems (H2D2).

Core Theme 5: Cultivate Security Awareness Culture

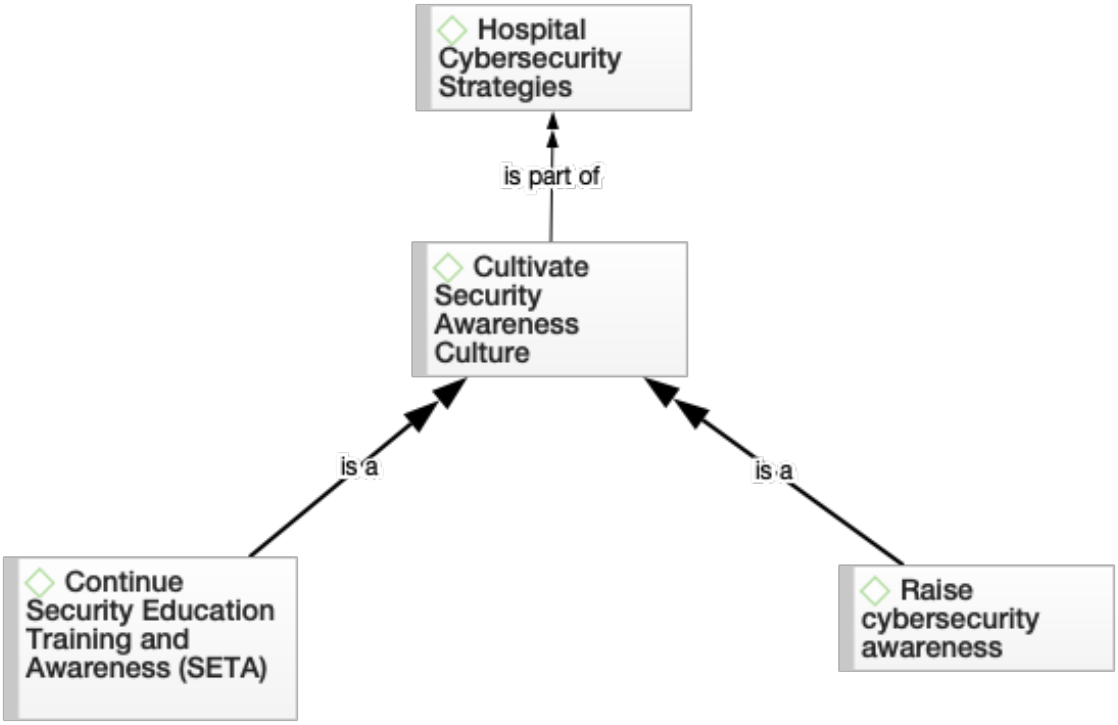
Cultivate security awareness culture was the fifth core theme of this study data. The core theme was in congruity with the RAT theory with particular emphasis on the criterion of a suitable target as it relates to having the employees unaware of the security culture. In creating a cybersecurity awareness culture, the c-executives and dedicated leaders must buy into the initiative at the beginning to succeed in the long run. Such leadership must be willing to hire trustworthy employees to maintain a cyber awareness culture. The InfoSec may ask the question of whether it is an inside job. For example, the hospital may employ individuals who commit an insider security incident because they

are potential offenders (whether motivated or not) close to suitable targets (healthcare data) without capable guardianship. The implementors of the cyber awareness culture assume that all the staff is committed to keeping the IT environment safe.

Cultivating a cyber security-aware culture was a pertinent and necessary subject for discussion in the literature review. A healthcare culture that communicates risks and threats information is as significant as IT infrastructure maintenance, such as upgrading old hardware and software, updating and patches, and taking charge of an overarching risk assessment of endpoints (Offner et al., 2020). For the hospital, a third-party vendor prepared a vibrant, inclusive, security, and privacy-focused culture that started from the employees' hiring and onboarding and continued into a cyber awareness culture (H2D4). P4 shared that they have a monthly newsletter, wherein the current culture is stimulated by being made aware of the constant threats coming out. Communicating the information to their end-users without creating an alarm is imperative. They present the information, not in a technical form but more of an awareness form (high level) for them to understand. According to Georgiadou et al. (2022), a robust and healthy cyber culture is one whereby the individuals are knowledgeable about cybersecurity threats, are open to IT technology and process mechanisms, and feel emboldened to change their conduct to help protect themselves and others in the organization. Figure 10 displays an ATLAS.ti semantic network that represents the core theme 5.

Figure 10

Core Theme 5: Cultivate Security Awareness Culture



As shown in Figure 10, two emergent subthemes evolved from the data analysis into the core theme. Table 13 shows that six participants (68%) divulged information that generated codes used in mapping the cultivate security awareness culture core theme.

Table 14

Frequency of Participants (Max n = 9) Using Subtheme for Cultivate Security Awareness Culture

Subtheme	*n*	% of the frequency of participants
Continue security education training and awareness	6	68%
Raise cybersecurity awareness	6	68%
Documents	14	44%

Note. *n* = frequency of participants.

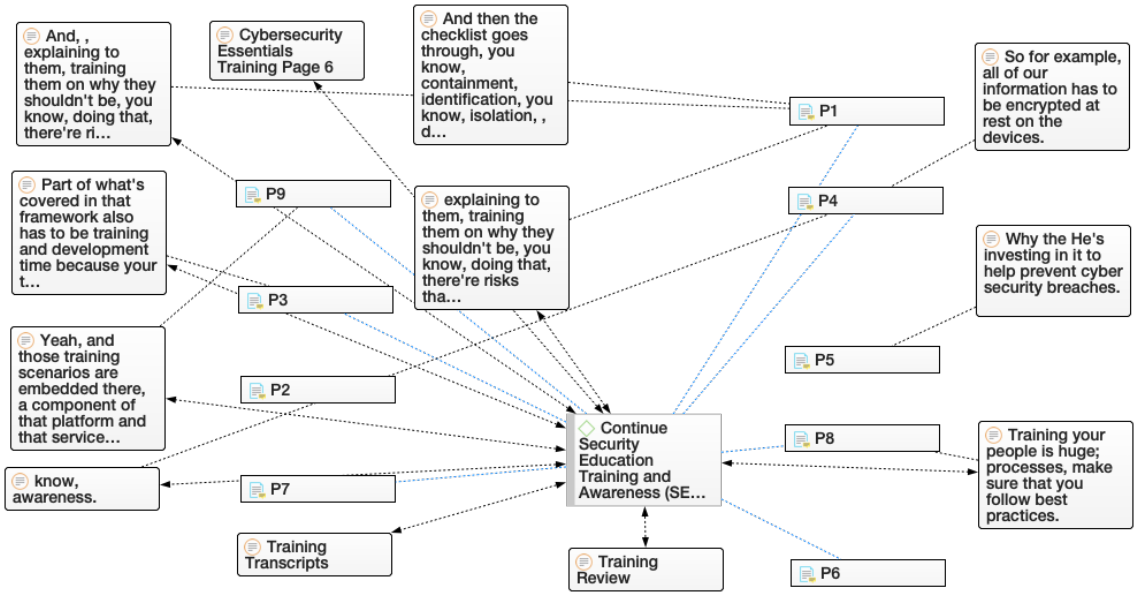
Subtheme 5.1: Continue Security Education, Training, and Awareness (SETA)

Continue security education, training, and awareness (SETA) surfaced as the first subtheme of cultivating a cybersecurity awareness culture. This subtheme aligned with the RAT conceptual framework, the lens that guides this study. The absence of a guardian is replaced by the opposite in the trio criteria (a motivated offender, a suitable target, and the absence of a guardian). As opposed to the guarding presence, the replacement criterion protects the IT environment and the employees who continue to participate in security education, training, and awareness (SETA). This subtheme permeates the literature review. Of the 9 participants, 7 joined the conversation on continued security education training and awareness (SETA). IT Information Security provided mandatory InfoSec, education, training, and awareness to all staff members on practicing their roles and responsibilities in protecting the hospital's sensitive data (H1D1, H1D3, H1D4, H2D2, H2D3, H3D1, & H3D17). P3 from Hospital-1 stated that their cyber framework covered training and development time because their teams must give time to train and to

stay current in technologies. P4 from Hospital-2 stressed that they continue to heighten the awareness and understanding of cybersecurity from the end-user perspective. P9 from Hospital-3 pointed out that one of their cyber tools has a unit for user awareness training whereby they send emails that look like phishing. Figure 11 displayed a network map of the continued security, education, training, and awareness (SETA) subtheme containing codes and participant quotations.

Figure 11

Subtheme 5.1: Continue Security, Education, Training, and Awareness



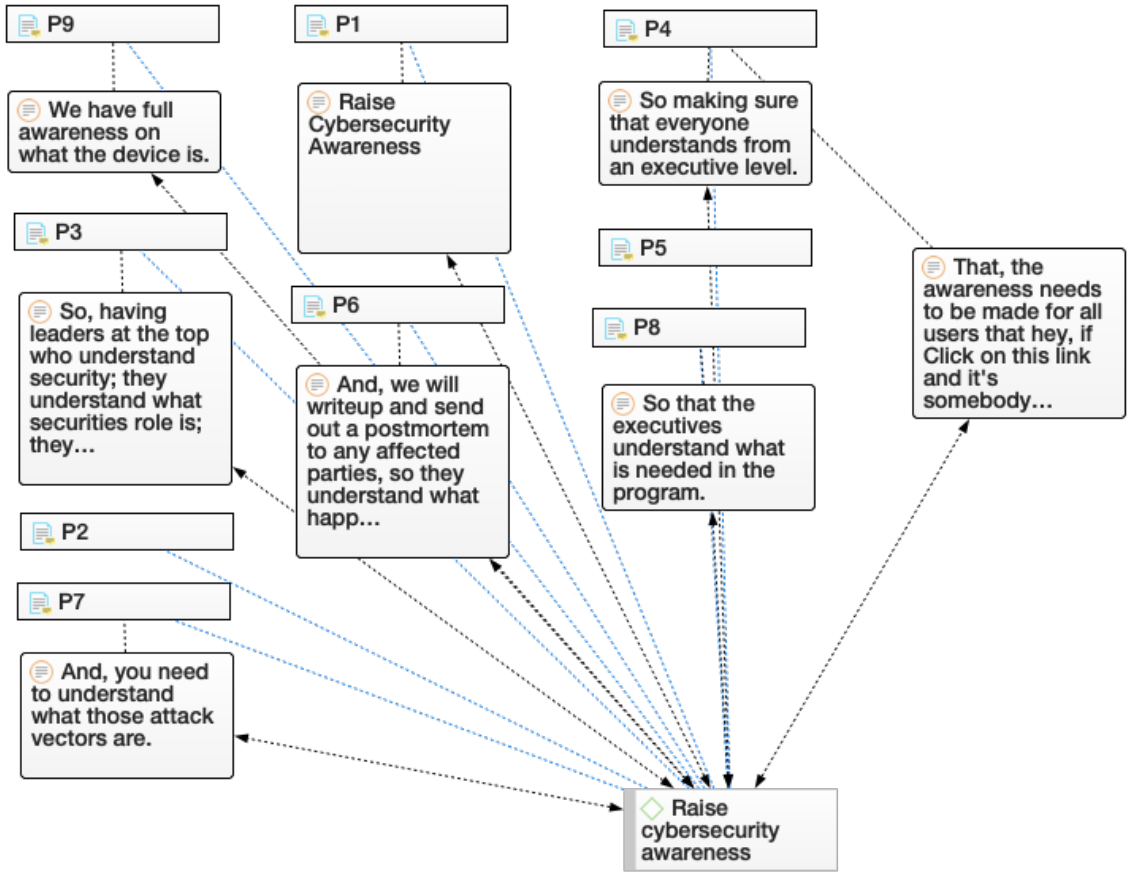
Continue security, education, training, and awareness is a feature of cultivating a security awareness culture that is highlighted in the literature review. Seventy-eight percent of the participants agreed with Hu et al. (2021) when they declared that security education, training, and awareness (SETA) is one of the most shared and predominant strategies for organizational security best practices.

Subtheme 5.2: Raise Cybersecurity Awareness

Seventy-eight percent of the research participants mentioned the need to raise cybersecurity awareness to cultivate a security awareness culture in the hospitals. Figure 12 shows a network map of the raised cybersecurity awareness subtheme comprising codes and participant quotations.

Figure 12

Subtheme 5.1: Raise Cybersecurity Awareness



Since humans are the weakest link in cybersecurity, hospitals' cybersecurity strategies should be cognizant of the necessity of raising cyber awareness among each end-user. Hart et al. (2020) posited that as a primary risk mitigation policy, hospitals are

budgeting and spending a significant amount of funds on professional training classes for their workers to raise awareness of the cybercriminals' assaults on the IT environment. Employers must invest in the employees, for they ought to understand cybersecurity (P8). Documents H1D3 and H3D5 correlated with the directive that security and privacy is a moving target, and hospitals recognize that dedicated employee involvement is a primary means of raising awareness. P3 and P6 stipulated that they have leaders at the top who understand information security and know what security's roles are. Moreover, they understand the role of protecting the hospital and its data (P3 and P6). Furthermore, they drive policies and procedures to match specific regulations or best practices. (P3 and P6). The success of any organization-wide program depends on the buy-in of the C-executives, for they need to understand and embrace the cybersecurity initiative. P4 concurred when they said making sure that everyone understands from the executive level. P9 summed it up nicely by saying cybersecurity awareness is all over the place.

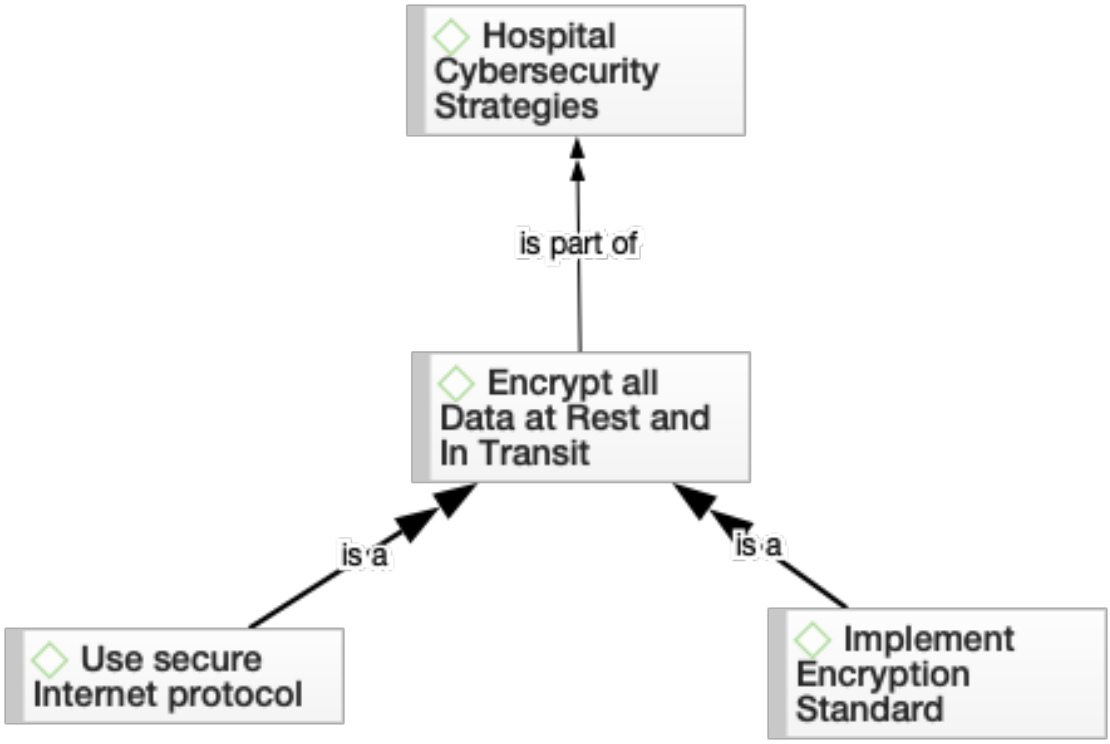
Core Theme 6: Encrypt All Data at Rest and in Transit

Encrypt all data at rest and in transit core theme was the next theme that emerged from the qualitative data analysis of the research data. This core theme is an integral part of the RAT conceptual framework because by encrypting the healthcare data, the hospital is guarding the sensitive data from motivated offenders who see the data as a suitable target. With encryption data, the motive is always to protect the healthcare data (at rest, in transit, or in use), RAT may be adapted to this digital environment of data encryption because the purpose is to prevent hackers and other cybercriminals from gaining access to sensitive data (PII, PHI). Moreover, within this context RAT explains cybercrimes

such as data loss and identity theft. Eichelberg et al. (2020) endorsed the strategy that encryption is one of the most prevalent best practices used in hospitals, primarily because the data at rest, in transit, or in use is profitable to the cybercriminals but detrimental to the victims. Figure 13 shows an ATLAS.ti semantic network representation of the emergence of core theme 6.

Figure 13

Core Theme: Encrypt All Data at Rest and in Transit



As shown in Figure 13, two emergent subthemes, use secure internet protocol subtheme and implement standard encryption subtheme, surfaced from the data analysis into the core theme 6. Table 14 shows that 4 participants (44%) communicated

information that resulted in codes used in mapping the surfacing of the use secure internet protocol subtheme. Nine participants (100%) expressed information cultivated in codes used to map the emergence of implement encryption standard subtheme. In the analysis, I used 11 documents (34%).

Table 15

Frequency of Participants (Max n = 9) Encrypt All Data at Rest and in Transit Core Theme

Subtheme	*n*	% of the frequency of participants
Use secure internet protocol	4	44%
Implement encryption standard	9	100%
Documents	11	34%

Note. *n* = frequency of participants.

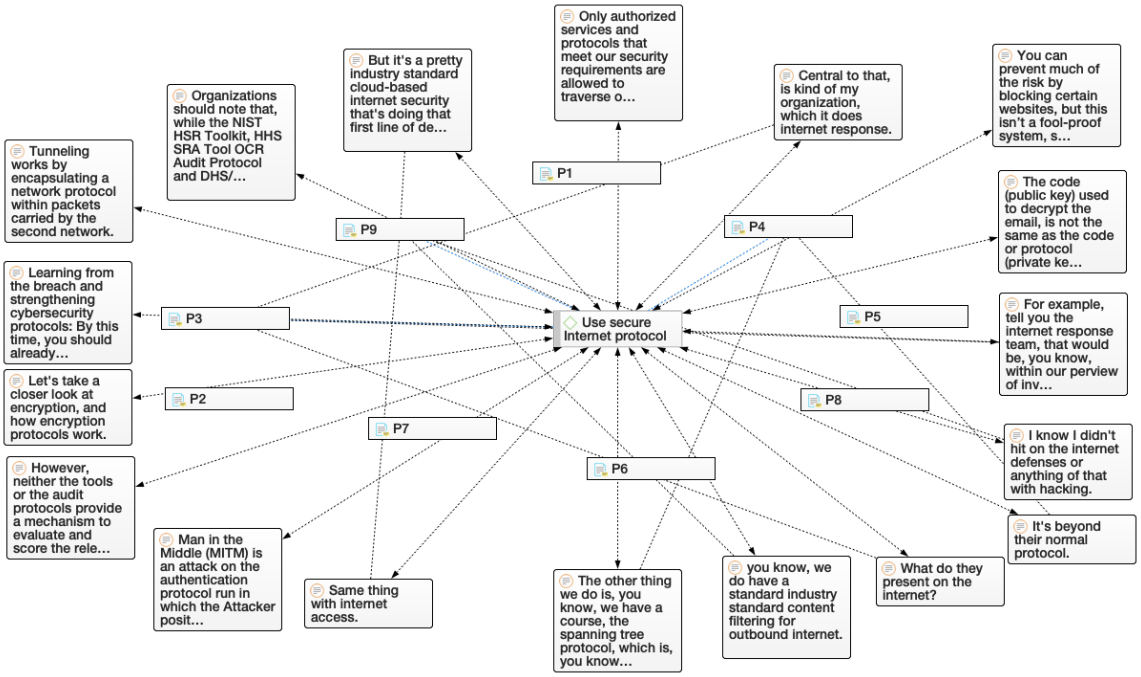
Table 14 depicted that forty-four percent of the participants shared information on use secure internet protocol subtheme. In comparison, one hundred percent of the participants submitted a response that covered the implement encryption standard subtheme. In the analysis, I used the 11 documents (34%). Information from H1D5, H2D3, and H3D5 read that the rationale to keep secure information triggered cryptographic algorithms to encrypt data at rest and in transit, such as email messages, to prevent interruption of IT delivery services.

Subtheme 6.1: Use Secure Internet Protocol

Four of the nine (44%) research participants mentioned using secure Internet protocol. According to Shaik and Alowaidi (2022), hypertext transfer protocol secure (HTTPS) encrypts all the Short Message Service (SMS) transferred between a patient's smartphone and Trusted Platform Module (TPM) at the hospital. Secure transmissions use Transport Layer Security (TLS) to establish a secure tunnel between patients. Tunneling, a secure communication protocol, works by encapsulating a network protocol within packets carried by the second network (H1D5). In response to the increased workforce working from home, many hospitals must address the prevalent use of VPN, secure tunneling. P3 explained that they have an Internet response team that uses secure Internet protocol to investigate an incident with specific guidelines involving their run books that address several security layers of different aspects of cybersecurity. Figure 14 shows a network map of the use secure Internet protocol containing codes and participants' quotations.

Figure 14

Subtheme: Use Secure Internet Protocol



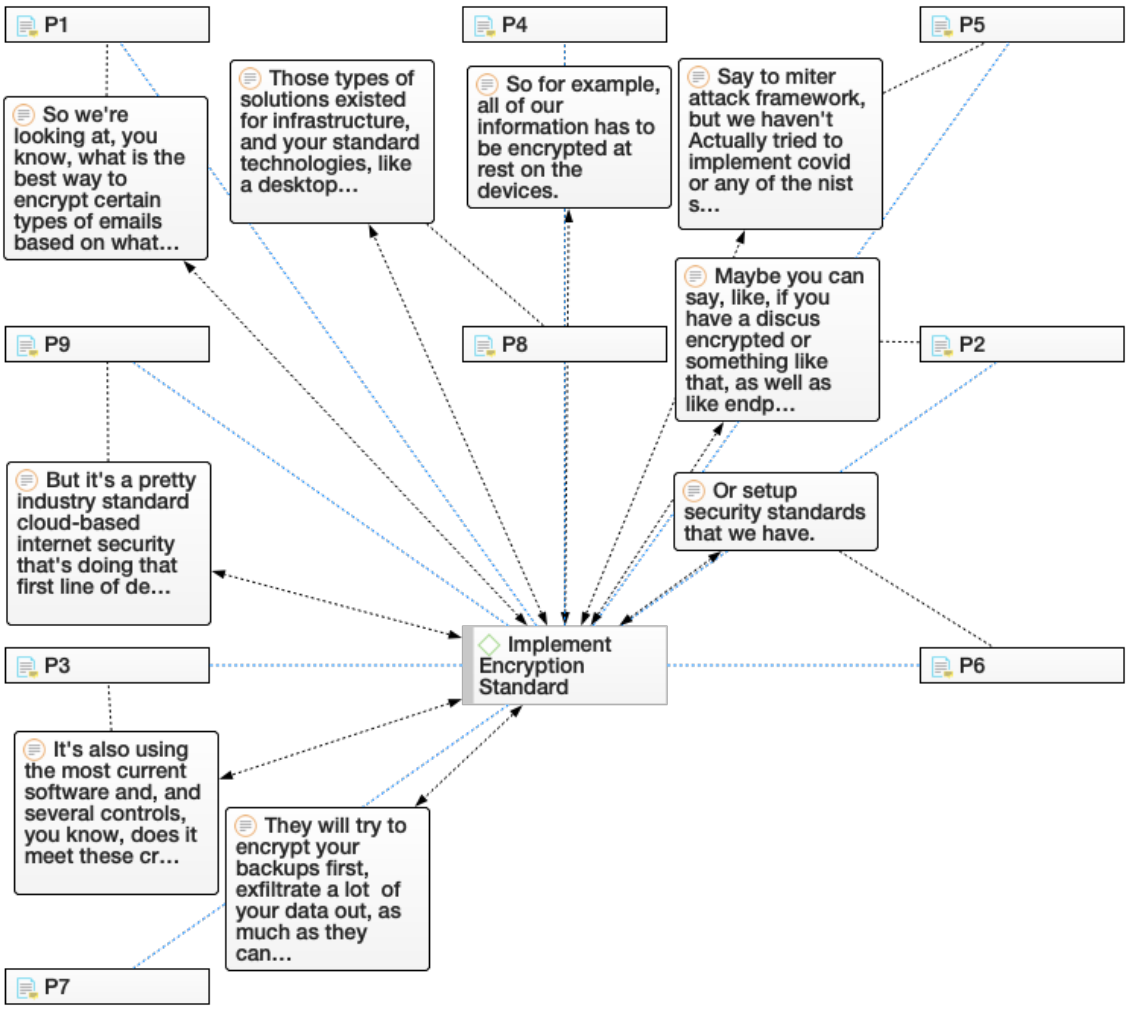
Thirty-three percent of the participants submitted information for review on the subtheme use secure Internet protocol. P9 pointed out that the end-user followed the process of surfing the Internet involves using the industry-standard cloud-based Internet security, which follows secure internet protocol because it is the first line of defense. The security design of the internet protocol, which is called IP Security, is a regulation of internet security. IP Security (IPSec) is a point-to-point protocol where one end encrypts, the other end decrypts, and both ends share security keys (Sani et al., 2019). All three hospitals use IPsec, a suite of protocols that secure Internet and network communication, and IPsec provides IT security services for TCP/IP protocol.

Subtheme 6.2: Implement Encryption Standard

The complete list of participants (9) subscribed to implement encryption standard, the second subtheme for encrypt all data at rest and in transit core theme, in their IT environment. Figure 15 displays a network map of implement encryption standard subtheme containing the participants' codes and quotations.

Figure 15

Subtheme: Implement Encryption Standard



Regarding the subtheme implement encryption standard, all the participants (100%) contributed to the discussion regarding the best practice to encrypt healthcare data. Because data at rest, in use, and in transit are critical and sensitive in hospitals' IT infrastructure, encryption is one of the most prevalent solutions used in hospitals (Eichelberg et al., 2020). All three hospitals in this study implement encryption standard on data collected from reading the participants' shared documents (H1D3, H2D1, H3D1), P1 discussed the best way to encrypt certain types of emails based on the data sent with those emails. P4 stipulated that all their data must encrypt at rest on the devices. P7 shared that they are Health Information Trust Alliance (HITRUST) Cybersecurity Framework (CSF) certified, and their standards include the implementation of encryption standards. P9 noted that their first line of defense against cybercriminal attacks is enforced by industry-standard encryption and cloud-based internet security.

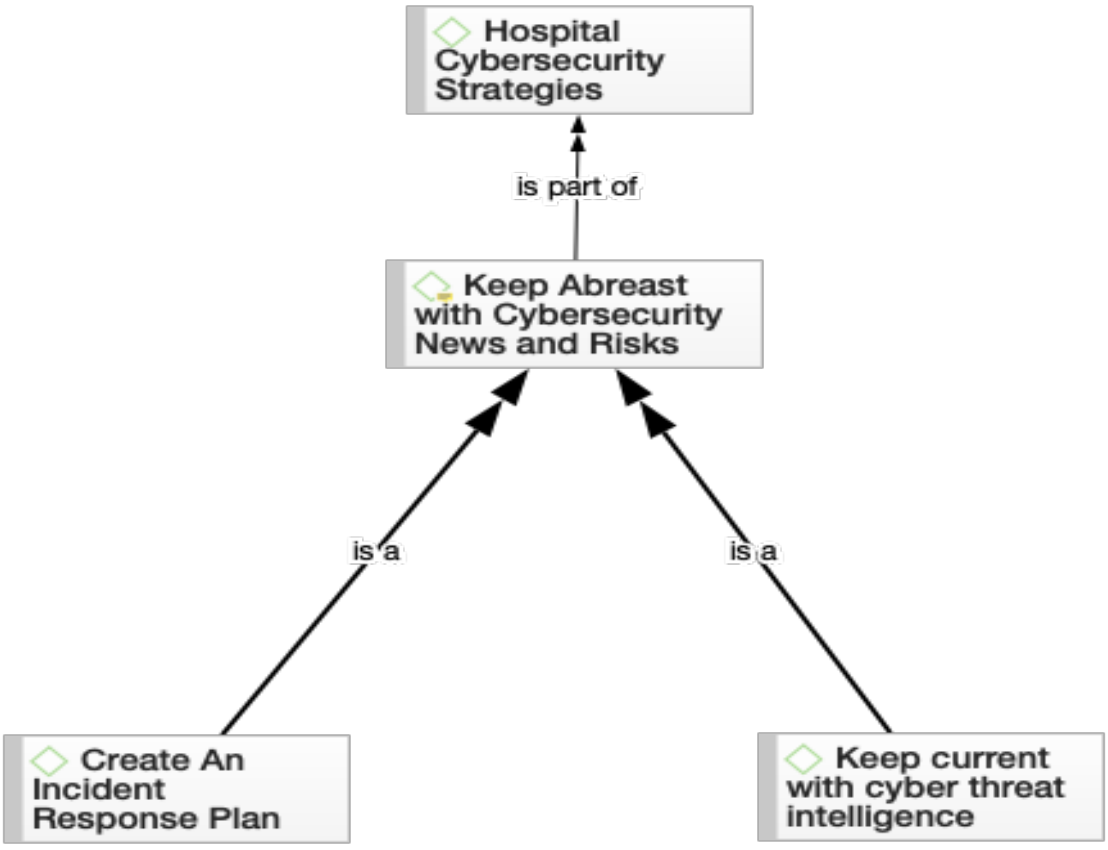
Core Theme 7: Keep Abreast With Cybersecurity News and Risks

Keep abreast with cybersecurity news and risks was the seventh core theme that surfaced from the study data. This core theme is congruent with the RAT conceptual framework. Being informed of potential threats and cyberattacks (cyber intelligence) to the hospital IT infrastructure allows the IT security managers to reduce cyber breaches such as phishing, hacking, malware, ransomware attacks, identity theft, and stealing PHI and PII. Such cybercriminal offenses, when examined within the RAT construct, happen when there is: (a) the presence of a likely offender, (b) the presence of a suitable target, and (c) the absence of a capable guardian (Felson, 1995) in cyberspace. Keep abreast (informed) with cyber news and risks subtheme permeates the literature review. While

hackers perfect their craft by using more complicated method and come up with more unaware ideas to attack hospitals, to keep their security processes up to date, it is incumbent on cybersecurity leaders to stay abreast on the most recent cyberattacks strategies and trends (Kim, 2018). Hospitals' InfoSec division could become unaware of significant updates that impact their IT infrastructure should they ignore cybersecurity development, risks, and news. Figure 16 displays an ATLAS.ti semantic network representation of the discovery of core theme 7.

Figure 16

Core Theme 7: Keep Abreast With Cybersecurity News and Risks



As displayed in Figure 16, two developed subthemes surfaced from the qualitative data analysis from the core theme 7. Table 15 shows seven participants (78%) who informed me of the strategies they use to reduce cybersecurity breaches at their hospitals. In the analysis, I used 7 documents (22%).

Table 16

Frequency of Participants (Max n = 9) Using Subthemes for Keep Abreast With Cybersecurity News and Risks Core Theme

Subtheme	*n*	% of the frequency of participants
Create an incident response plan	7	78%
Keep current with cyber threat intelligence	7	78%
Documents	7	22%

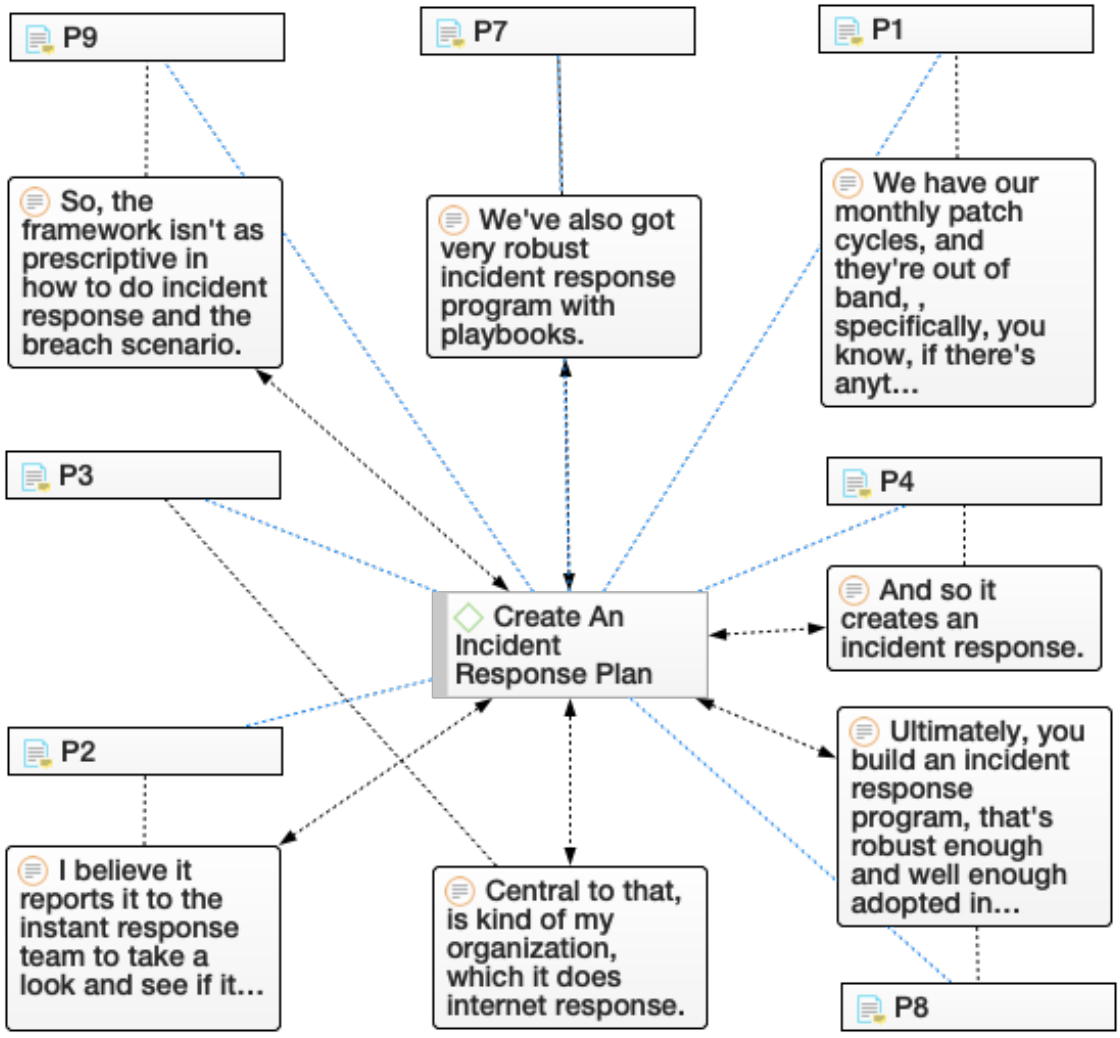
Note. *n* = frequency of participants.

Subtheme 7.1: Create an Incident Response Plan

Seven of the nine participants argued about the necessity to create an incident response plan subtheme. Figure 17 shows a network map of creating an incident response plan subtheme that comprises codes and quotations from 78% of the participants.

Figure 17

Subtheme 7.1: Create an Incident Response Plan



Creating an incident response plan is a common tactic in the literature review. The adage that if one fails to plan, then one plans to fail is entirely appropriate in this case. Besides implementing technical strategies to reduce incidents (security breaches), many hospitals also accomplish an incident response plan to mitigate the negative impact of a cyberattack and rapidly restore IT infrastructure normalcy (Ahmad et al., 2020). All three hospitals' (cases) InfoSec acknowledged that they created an incident response plan to

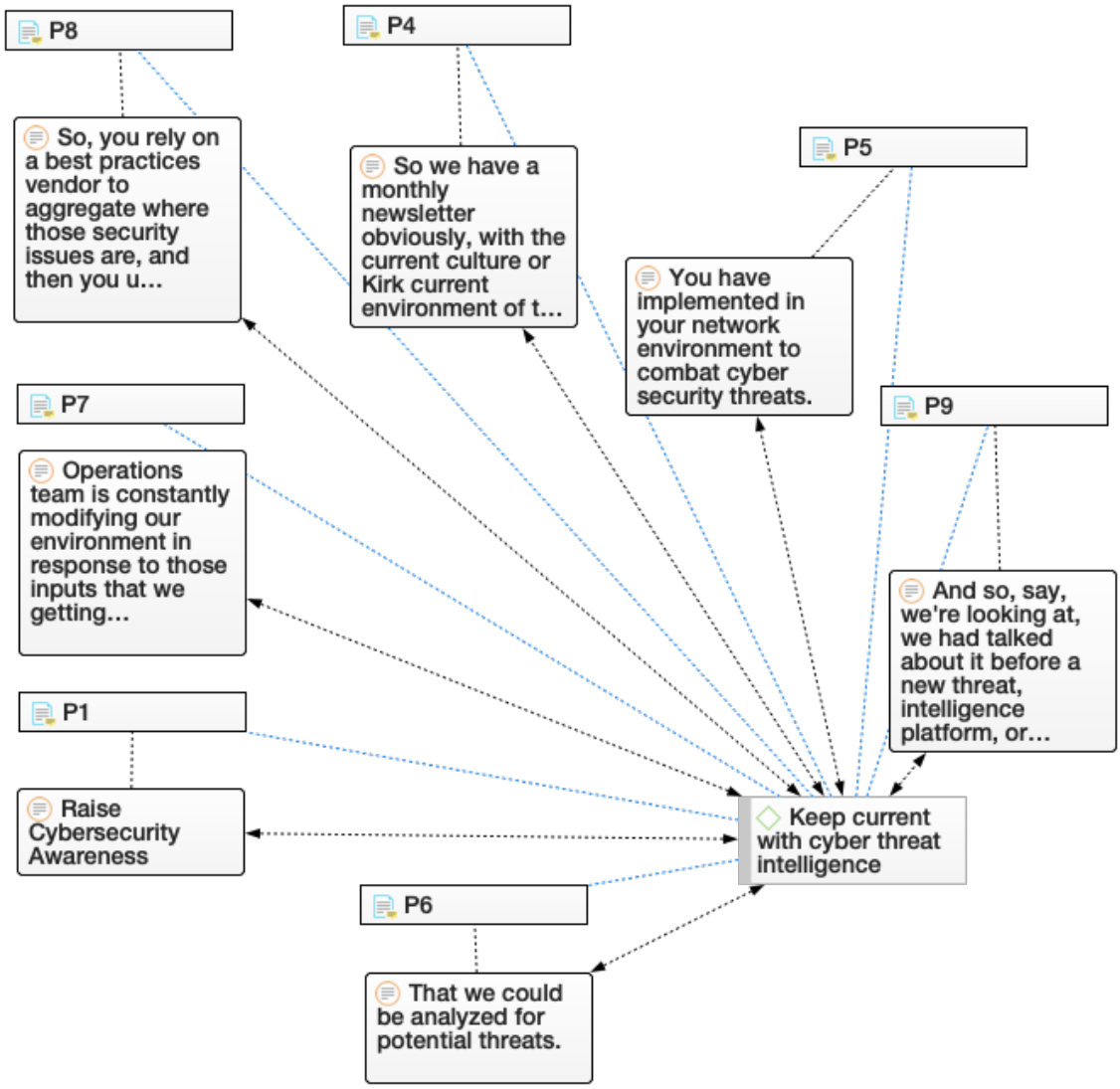
decrease the time it takes for the business to resume a satisfactory functional level (P1, P4, P7, P9). Hospital-3 IT implemented and maintained the business continuity and disaster recovery program for IT assets activated during disasters, emergencies, and other catastrophic or unplanned events that severely disrupt technology, physical assets, or workforce members (H3D20). P8 stated that ultimately, they build an incident response program that is robust enough and well enough to be adopted in their hospital to make it effective.

Subtheme 7.2: Keep Current With Cyber Threat Intelligence

Seventy-eight percent of the participants practice keeping current with the cyber threat intelligence subtheme presented in the literature review. This subtheme falls within the message of the RAT conceptual framework, which suggests that a crime is most likely to occur when the three criteria are present. Ibrahim et al. (2018) denoted cyber threat intelligence (CTI) as the constant habit of analyzing and consolidating incoherent cyber data to gather evidence-based information concerning an organization's (a hospital's) pertinent and potential threats. Figure 17 displays a network map of keeping current with the cyber threat intelligence subtheme comprising codes and participant quotations.

Figure 18

Subtheme 7.2: Keep Current With Cyber Threat Intelligence



Although many institutions are rapidly resorting to cyber threat intelligence (CTI) to facilitate them in deciding which vulnerabilities to tackle first, surviving CTI mechanisms frequently address the issues after the fact (Samtani et al., 2022). The increasing risk of cybercrimes resulted in many organizations transforming their cyber defense to be more proactive than reactive. To make an informed decision for the security of the hospital's IT infrastructure, IT leaders keep abreast of third-party vendors' curated

programs to leverage cyber compliance resources (H2D3). P8 explained that they rely on a best practices vendor to aggregate where those security issues are. Then they use that technology to scan their environment to ensure that they are keeping the environment up-to-date and protected from those newly emerging threats. P6 concurred with P8 that they analyzed for potential threats. P5 announced that they implemented in their network environment CTI to combat cybersecurity threats.

Applications to Professional Practice

Hospitals are constantly confronted with the ever-changing cyberthreats resulting in risky patient safety. Dameff et al. (2019) highlighted the importance of comprehending the workflow effect of cybersecurity controls in the hospital environment to prevent successful and malicious breaches of patients' sensitive data. Associating cybersecurity and patient safety will do two things: (a) help the hospital protect patient safety and privacy and (b) ensure unbroken effective delivery of excellent care by reducing threats or successful cyberattacks, therein erasing negative impact on healthcare operation. Information technology security managers who emulate the strategies unearth in this study should be able to reduce cyberattacks such as hacking, ransomware, malware, phishing, and insider threat to their hospital IT infrastructure. Successful cybersecurity strategies begin with a cultivated cyber awareness culture where all the workforces are committed to playing their part in securing the IT environment. The intent is not to eliminate the breaches but to minimize the impact on the functionality of the IT delivery services. To have a secure and safe IT environment, the IT security manager must implement comprehensive strategies to protect the workspace from malicious attacks.

Hence, the security countermeasures uncovered in this study, if implemented, will enhance the working milieu. Therefore, the IT security managers may implement the themes (best practices) to reduce the occurrence of successful cyberattacks, providing a trusted and trusting workspace.

The seven cybersecurity strategies that emerged from the data analysis of the participants' answers and documentation are: (a) ensure adherence to top cybersecurity framework, (b) implement adequate and effective cybersecurity controls (c) conduct regular cybersecurity risk assessment, (d) maintain an air gap technique backup, (e) cultivate security awareness culture, (f) encrypt all data at rest and in transit, and (g) keep abreast with cybersecurity news and risks. Blanke and McGrady (2016) purported that the healthcare industry has the most reported breaches, such as portable devices, physical breaches, and insider threats. Such incidents have security gaps that require prescriptive improvement based on the best practices, cybersecurity strategies. The IT security managers, such as CISOs, Directors of InfoSec, and CIOs, could apply the identified seven strategies to reduce cybersecurity breaches in their hospitals.

Hospitals are most vulnerable and targeted by cybercriminals' malicious attacks because they comprise tremendous information of valuable intelligence and monetary payoff to nation-state actors and cyber thieves. The prized data possess PHI, financial information from bank cards and bank account numbers, PII such as Social Security numbers, and intellectual property from medical research and development. On the dark web, the loot of patient health records may fetch up to 10 times or more than stolen credit cards number. Further, the cost to rectify a breach in a hospital is nearly three times

greater than in other industries. Subsequently, from this study, tremendous cost savings could result from putting in place the findings, such as encrypting data at rest and in transit to avoid violating the confidentiality, integrity, and availability of sensitive data.

Another risk to patient privacy resulted in hackers gaining access to sensitive information, including PHI, because of their successful cyberattacks on several systems such as electronic health records (EHR). At the same time, hospitals may suffer potential harm to their reputation within the hospital environment and experience violations of HIPAA's privacy and security rules that result from failure to maintain private patient records. Of utmost importance, the hackers may jeopardize the patient safety and delivery of their care. According to Gordon et al. (2017), cybersecurity is a progressively significant threat to healthcare delivery, and email phishing is a primary attack vector against hospital employees. The findings of this study are applicable to this situation when it detects and prevents or mitigates the attack vectors from penetrating the cyber security barriers.

When the IT personnel loses computer access to medical records and critical medical devices, ransomware holds them hostage, which results in ineffective patient care. Such inadequate patient care leads to severe impact on patient health and outcomes, and the success of the hackers will include stealing the information, and they may change the data. The IT security manager could use the air-gapped backup to recover from being held ransom by hackers. Besides avoiding the paying the expensive ransom, such timely and secure recovery could restore confidence in the stakeholders of the hospitals.

Implications for Social Change

A successful cybersecurity breach can cause significant damage to the hospitals' social community. Reducing these breaches can improve the lifestyle of patients and the community of the hospitals with all the stakeholders such as nurses, doctors, respiratory therapists, accountants, security guards, c-executives, multiple IT managers, and other essential staff. Trust is a significant value of patient care. Cyberattacks can destroy the hospital's reputation and undermine the patients' trust in the hospital staff. If the hospital IT leaderships were to apply the recommendations from this study to the hospitals, then such action would trigger patients' trust. For example, the safety of the patient's PHI would prevent identity theft.

Recommendations for Action

Qualitative data analysis of data collected from nine IT security managers in hospitals in the eastern United States and the ten provided documents spawned seven recommended action plans. According to Wirth (2017), understanding the economics of cybersecurity and its impact on hospitals, IT security managers need to know how the clandestine economy works, the detrimental financial meaning of a successful cyberattack, and the role of c-executives is crucial to tackle cyber risk and reducing any threat. IT security managers at hospitals could consider the seven strategies as recommendations to reduce cybersecurity breaches in their hospitals. The seven recommendations are courses of action of the study findings, which are: (a) ensure adherence to top cybersecurity framework, (b) implement adequate and effective cybersecurity controls, (c) conduct regular cybersecurity risk assessment, (d) maintain an

air gap technique backup, (e) cultivate security awareness culture, (f) encrypt all data at rest and in transit, and (g) keep abreast with cybersecurity news and risks.

First, I recommend to IT security managers in hospitals to ensure adherence to top cybersecurity frameworks, such as ISO/IEC 27001, NIST 800-53, or HITRUST CSF, as a strategy to reduce cyber incidents. Moreover, these frameworks or CSFs are constructed to add the missing guidance of the hospital business and cybersecurity processes. In addition, they can help IT personnel apprehend security status, establish, or improve a cybersecurity construct, communicate cyber constraints with stakeholders, and identify circumstances for updated standards. Furthermore, these CSFs must adapt cyber policies and procedures to fit their IT infrastructure within the hospital environments. The IT security managers should use the right tool to create policies and procedures that align with the best practices covered in the CSFs.

Second, to stand up the best practice defense system against cybersecurity cybercriminal attacks of ransomware, malware, and hacking, I recommend to the IT security manager to implement adequate and effective cybersecurity controls such as (a) keep the patching of operating systems and other applications up to date, (b) implement user two-factor or multifactor authentication, (c) protect healthcare data, (d) protect access with efficient identity management, and (e) ensure strong password. To minimize cybersecurity risk, IT security managers in hospitals should deploy a proactive attitude to software security patch management. The notion is to reduce a security incident before it happens. IT security professionals should implement two-factor or multifactor authentication in their hospitals' environments because it is fundamental to cyber security

since it guarantees nullification of the risks related to compromised passwords. I endorse protecting of healthcare data from unauthorized access, use, and disclosure. The IT security managers could accomplish the cybersecurity goals of the CIA triad. These managers should implement identity management which involves an IAM framework to control user access to critical information within the hospitals. Most importantly, creating a strong password is an essential procedure to protect users on the on-prim network and the Internet. Therefore, using a long and complex password is one of the strongest ways to defend the IT infrastructure.

According to Ayatollahi and Shagerdi (2017), concerning the information security strategies used in the hospitals, the use of the cyber controls was the most important; hence, the high probability risk assessment require sooner than later corrective actions. Against such a backdrop, I propose my third recommendation to the IT security manager to conduct a regular cybersecurity risk assessment. Therefore, the underpinning causes of such potential risks should be found and monitored before the hospital experience any detrimental and costly results. Argaw et al., 2020 suggested cybersecurity risk assessment is dependent on knowing the at-risk hospital assets, which is a foundation standard for real-time IT infrastructure, and it uses the process of vulnerability management to filter out the threats. Therefore, IT security managers should perform regular cyber risk assessment because the process identifies the different information assets that are potential targets of cyberattacks, such as systems, software, laptops, hardware, intellectual property, laptops, and customer data. Subsequently, the mechanism identifies the risks likely to impact those assets.

The fourth recommendation for IT security managers is to maintain an air gap technique backup, an offline backup of the healthcare data that must be unreachable by hackers and other cybercriminals. Many hospitals have become victims of ransomware situations; therefore, any storage is readily available by infected servers is prime target that will result in data violation. Hence, the primary strategy to recover involves keeping air gap backups that will provide a replacement for the hacker's stolen healthcare data.

Fifth, I recommend to the IT security manager of hospitals to cultivate a security awareness culture. The notion of cybersecurity culture denotes the mindsets, understanding, presuppositions, standards, and values of the staff of an organization as it relates to cybersecurity (Veksler et al., 2018). Therefore, the cyber awareness culture means the hospital workplace has a cyber culture that the workforce practices daily. The proven and tried cyber strategy is cultivating a cyber awareness culture in the IT environment. Hence, IT security managers should improve cybersecurity at the hospitals or healthcare industry, use cybersecurity training to create a culture whereby everyone embraces the idea that cyber safety is part of their responsibility, and they possess the know-how to protect the hospital data, apps, and IT environment.

Sixth, I recommend that all IT security managers of the hospitals encrypt all data at rest, in transit, and in use. If all cybersecurity defense systems fail, then the last line of defense is to have the healthcare data encrypted so that even if the cybercriminals get to it, it would be useless to them because they do not have the decryption keys to make it accessible. InfoSec should protect healthcare data in transit and at rest so that data confidentiality, integrity, and availability can be preserved (Karunarathne et al., 2021).

Although data at rest is often less vulnerable than the data in transit, cybercriminals prefer data at rest because it is more valuable than other industries' data, and it generally has critical sensitive information. Hence, IT security managers could benefit by encrypting this crucial data. Equally important, the InfoSec managers could encrypt the data before the transfer, authenticate the endpoints, and decrypt and verify the data upon arrival.

The seventh and final recommendation I have for the hospital IT security managers is to keep abreast with cybersecurity news and risks. Going forward, they need to be on the cutting edge of cybersecurity information and be thoroughly prepared for any cyberattack from any angle. The modified adage is that it is not a question of if the hospitals will have a cyber incident but when will the cybersecurity breaches happen. According to Esteves et al. (2017), the singular solution to tackle current cybersecurity threats is to maintain up-to-date protective processes, incessantly train personnel, keep abreast of the state of information security, and utilize controlled-enabled tools to detect preemptively, analyze and react to incidents. Knowing and understanding these precise recommendations, IT security managers should stay informed about cybersecurity because: (a) cybersecurity impacts are expected, (b) hacking happens more often than realized, and (c) both technology and hackers are evolving rapidly. Subsequently, the IT security managers may stay informed through these recommendations: (a) read up on cybersecurity on blogs or online news and (b) employ IT professionals to keep the hospital IT organization informed and secured.

The IT professionals who will find the results of this study helpful include the Chief Information Officer (CIO,) CISO, Director of InfoSec, and other IT Security Managers. Prospective researchers may use this study findings as a foundation to generate future researchers and contribute to the field of study, Cybersecurity in different organizations. I will share the study's findings through: (a) training webinars, (b) business and scholarly journals, (c) training seminars, (d) video conferencing and workshops, (e) classes in hospital training, tabletops and simulations, and (d) colleges and universities lectures.

Recommendations for Further Study

Presently, any cybersecurity researcher is presented with a fantastic opportunity to dig into the wealth of opportunities. The target of what cybersecurity is and how it works are coming to focus. However, the research community's challenges are more complex than before and changing rapidly. Therefore, I recommend an interdisciplinary research approach such as Artificial Intelligence and Cybersecurity as it relates to the internet of things (IoT). Other disciplines such as sociology, anthropology, economics, mathematics, and similar subjects are enhancing the research agenda, which will trigger guidance on effectively implementing cybersecurity strategies for the reduction of successful cyber-attacks. Prospective researchers could use a different population, such as stakeholders in banking or other financial institutions.

Reflections

During my journey at Walden University, I developed a renewed respect for previous scholars; I am stunned by the high demand of time and effort to complete the

Doctor of Information Technology (DIT). My understanding of the online education process has evolved, and I learned much about cybersecurity implementation in the hospital's IT environment.

I am surprised how much resilience is necessary for surviving the multiplicity of attempts to get approval for the letter of cooperation from the C-executives at hospitals during the Covid-19 pandemic. The Covid-19 pandemic presented a barrier, resistance, and refusal by the business leaders because of the shifted priority to deliver IT services to stakeholders working from home and on the premises of the hospitals. The leaders were preoccupied with responding to the needs created by the remote workforce. Although business continuity plans are intended to address operational events such as natural disasters, cybersecurity breaches, and power outages, IT personnel were unprepared for a global health emergency. Business continuity planning presented an uncertainty that made my requests a low priority.

Summary and Study Conclusions

My primary goal was to unearth useful strategies to minimize the impact of cybersecurity breaches in the milieu of high functional hospitals' IT infrastructure. To reduce cybersecurity threats in hospitals, the IT security managers should implement tried and proven cyber strategies (best practices) as emerged in this study. Hospitals' IT infrastructure continues to require cybersecurity measures because cybersecurity of hospitals is not only critical to hospitals' operations but, first and foremost, to patients' safety. I consider cybersecurity as one of the most essential features of the rapid growing digital world. Using of the RAT conceptual framework as a foundation to study the

research problem, strategies surfaced from the data analysis process to answer the research question for this qualitative exploratory multiple case research.

Seven strategies for the reduction of cybersecurity breaches in hospitals were: (a) ensure adherence to top cybersecurity framework, (b) implement adequate and effective cybersecurity controls, (c) conduct regular cybersecurity risk assessment, (d) maintain an air gap technique backup, (e) cultivate security awareness culture, (f) encrypt all data at rest and in transit, and (g) keep abreast with cybersecurity news and risks. All seven of the cybersecurity strategies aligned to the RAT conceptual constructs. The primary recommendation from this study's findings suggest that hospitals need to implement the seven cyber strategies (best practices) to reduce cybersecurity breaches and minimize cybercriminal incidents (cyberattacks). Implementing such strategies could reduce cyber breaches in the IT environment in hospitals and positively affect social change within the healthcare community for the patients and other stakeholders. The findings from this study are now subject to further research by potential researchers to contribute to detecting and reducing cybersecurity breaches in hospitals.

References

Ab Rahman, N. H., Kessler, G. C., & Choo, K. K. R. (2017). Implications of emerging technologies to incident handling and digital forensic strategies: A routine activity theory. In K. K. R. Choo & A. Dehghantanha (Eds.), *Contemporary digital forensic investigations of cloud and mobile applications* (pp. 131-146). Elsevier. https://doi.org/10.1016/B978-0-12-805303-4.00009-5

Agustina, J. R. (2015). Understanding cyber victimization: Digital architectures and the disinhibition effect. *International Journal of Cyber Criminology*, *9*(1), 35-54. https://doi.org/10.5281/zenodo.22239

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, *71*(8), 939-953. https://doi.org/10.1002/asi.24311

Akers, R. (1997). *Criminological theories: Introduction and evaluation* (2nd ed.). Roxbury. https://doi.org/10.2307/1319175

Akers, R. (1998). *Social learning and social structure: A general theory of crime and deviance.* Northeastern University Press. https://doi.org/10.4324/9781315129587

Allred, P. D., Maxwell, G. M., & Skrla, L. (2017). What women know: Perceptions of seven female superintendents. *Advancing Women in Leadership*, *37*, 1-11. http://scholarlycommons.pacific.edu/ed-facarticles

Alshamaila, Y., Papagiannidis, S., & Li, F. (2013). Cloud computing adoption by SMEs in the north east of England. *Journal of Enterprise Information Management*, 26(3), 250-275. https://doi.org/10.1108/17410391311325225

Andrasik, M. P., Chandler, C., Powell, B., Humes, D., Wakefield, S., Kripke, K., & Eckstein, D. (2014). Bridging the divide: HIV prevention research and black men who have sex with men. *American Journal of Public Health*, *104*(4), 708-714. https://doi.org/10.2105/ajph.2013.301653

Andresen, M. A. (2011). Estimating the probability of local crime clusters: The impact of immediate spatial neighbors. *Journal of Criminal Justice*, *39*(5), 394-404. https://doi.org/10.1016/j.jcrimjus.2011.05.005

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in human behavior*, *69*, 437-443. https://doi.org/10.1016/j.chb.2016.12.040

Anyan, F. (2013). The influence of power shifts in data collection and analysis stages: A Focus on qualitative research interview. *Qualitative Report*, *18*, Article 36. https://doi.org/10.46743/2160-3715/2013.1525

Arcuri, M. C., Brogi, M., & Gandolfi, G. (2017). How does cyber crime affect firms? The effect of information security breaches on stock returns. In A. Armando, R. Baldoni, & R. Focardi (Eds.), *Proceedings of the First Italian Conference on Cybersecurity (ITASEC17*), *Venice, Italy* (pp. 175-193). http://ceur-ws.org/Vol-1816/paper-18.pdf

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J. M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, *20*(1), 1-10. https://doi.org/10.1186/s12911-020-01161-7

Astani, M., & Ready, K. J. (2016). Trends and preventive strategies for mitigating cybersecurity breaches in organizations. *Issues in Information Systems*, *17*(2), 208-214.

Ayatollahi, H., & Shagerdi, G. (2017). Information security risk assessment in hospitals. *The open medical informatics journal*, *11*, 37-43 https://doi.org/10.2174%2F1874431101711010037

Baranchuk, A., Refaat, M. M., Patton, K. K., Chung, M. K., Krishnan, K., Kutyifa, V., Upadhyay, G., Fisher, J. D., Lakkireddy, D. R., & American College of Cardiology's Electrophysiology Section Leadership. (2018). Cybersecurity for cardiac implantable electronic devices: What should you know?. *Journal of the American College of Cardiology*, *71*(11), 1284-1288. https://doi.org/10.1016/j.jacc.2018.01.023

Barclay, C. (2014). Sustainable security advantage in a changing environment: The cybersecurity capability maturity model (CM2). In *Proceedings of the 2014 ITU Kaleidoscope Academic Conference: Living in a Converged World— Impossible Without Standards?* (pp. 275–282). International Telecommunication Union. https://doi.org/10.1109/kaleidoscope.2014.6858466

Barnham, C. (2015). Quantitative and qualitative research. *International Journal of Market Research, 57*, 837–854. https://doi.org/10.2501/IJMR-2015-070

Bauman, S., & Yoon, J. (2014). This issue: Theories of bullying and cyberbullying. *Theory Into Practice,* 53(4), 253-256. https://doi.org/10.1080/00405841.2014.947215

Baur, X., Budnik, L. T., Ruff, K., Egilman, D. S., Lemen, R. A., & Soskolne, C. L. (2015). Ethics, morality, and conflicting interests: how questionable professional integrity in some scientists supports global corporate influence in public health. *International journal of occupational and environmental health*, *21*(2), 172-175. https://doi.org/10.1179/2049396714Y.0000000103

Beauregard, E., Rossmo, D. K., & Proulx, J. (2007). A descriptive model of the hunting process of serial sex offenders: A rational choice perspective. *Journal of Family Violence*, *22*(6), 449-463. https://doi.org/10.1007/s10896-007-9101-3

Beck, C. D. (2014). Antecedents of servant leadership: A mixed methods study. *Journal of Leadership & Organizational Studies*, *21*(3), 299-314. https://doi.org/10.1177/1548051814529993

Bekhet, A. K., & Zauszniewski, J. A. (2012). Methodological triangulation: An approach to understanding data. *Nurse researcher*. https://doi.org/10.7748/nr2012.11.20.2.40.c9442

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2015.01.039

Benzel, T. (2015). A strategic plan for cybersecurity research and development. *IEEE Security & Privacy*, *4*(August), 3–5. https://doi.org/10.1109/MSP.2015.84

Berger, R. (2015). Now I see it, now I don't: Researcher's position and reflexivity in qualitative research. *Qualitative research*, *15*(2), 219-234. https://doi.org/10.1177/1468794112468475

Berglund, H. (2015). Between cognition and discourse: phenomenology and the study of entrepreneurship. *International Journal of Entrepreneurial Behavior & Research*, *21*(3), 472-488. https://doi.org/10.1108/IJEBR-12-2013-0210

Bernik, I., & Prislan, K. (2016). Measuring information security performance with 10 by 10 model for holistic state evaluation. *PLoS ONE, 11(9)* e0163050. https://doi.org/10.1371/journal.pone.0163050

Berry, L. E. (2016). The research relationship in narrative enquiry. *Nurse Researcher*, *24*(1). https://doi.org/10.7748/nr.2016.e1430

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. https://doi.org/10.1177/1049732316654870

Blake, L., Francis, V., Johnson, J., Khan, M., & McCray, T. (2017). Developing robust data management strategies for unprecedented challenges to healthcare information. *Journal of Leadership, Accountability, and Ethics*, *14*(1), 22-31. https://articlegateway.com/index.php/JLAE/about

Blanke, S. J., & McGrady, E. (2016). When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: A

cybersecurity risk assessment checklist. *Journal of healthcare risk management*, *36*(1), 14-24. https://doi.org/10.1002/jhrm.21230

Boblin, S. L., Ireland, S., Kirkpatrick, H., & Robertson, K. (2013). Using Stake's qualitative case study approach to explore implementation of evidence-based practice. *Qualitative health research*, *23*(9), 1267-1275. https://doi.org/10.1177/1049732313502128

Boddy, C. R. (2016). Sample size for qualitative research. *Qualitative Market Research: An International Journal*, *19*(4), 426-432. 10.1108/QMR-06-2016-0053. https://doi.org/10.1108/qmr-06-2016-0053

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., & Cotton, S. (2015). Determinants of Online Safety Behaviour: Towards an Intervention Strategy for College Students. Behaviour & Information Technology 34 (10): 1022–1035. https://doi.org/10.1080/0144929X.2015.1028448

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative research journal*, *9*(2), 27. https://doi.org/10.3316/QRJ0902027

Brantingham, P. L., & Brantingham, P. J. (1993). Nodes, paths and edges: Considerations on the complexity of crime and the physical environment. *Journal of environmental psychology*, *13*(1), 3-28. https://doi.org/10.1016/S0272-4944(05)80212-9

Bunch, J., Clay-Warner, J., & Lei, M. K. (2015). Demographic characteristics and victimization risk testing the mediating effects of routine activities. *Crime & Delinquency, 61*, 1181–1205. https://doi.org/10.1177/0011128712466932

Burns, A. J., Johnson, M. E., & Honeyman, P. (2016). A brief chronology of medical device security. *Communications of the ACM*. https://doi.org/10.1145/2890488

Califf, R. M., & Sugarman, J. (2015). Exploring the ethical and regulatory issues in pragmatic clinical trials. *Clinical Trials*, *12*(5), 436-441. https://doi.org/10.1177/1740774515598334

Campbell, R., & Ahrens, C. E. (1998). Innovative community services for rape victims: An application of multiple case study methodology. *American Journal of Community Psychology*, *26*, 537-571. https://doi.org/10.1023/A:1022140921921

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014, September). The use of triangulation in qualitative research. In *Oncology nursing forum* (Vol. 41, No. 5). https://doi.org/10.1188/14.ONF.545-547

Cavelty, M. D. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and Engineering Ethics*, *20(3)*, 701–715. https://doi.org/ 10.1007/s11948-014-9551-y

Chandna, V., & Tiwari, P. (2021). Cybersecurity and the new firm: surviving online threats. *Journal of Business Strategy*. https://doi.org/10.1108/JBS-08-2021-0146

Chaudhry, S. A., Naqvi, H., Shon, T., Sher, M., & Farash, M. S. (2015). Cryptanalysis and improvement of an improved two factor authentication protocol for telecare medical information systems. *Journal of Medical Systems*, *39*(6), 66. https://doi.org/10.1007/s10916-015-0244-0

Chen, Y. A. N., Ramamurthy, K. R. A. M., & Wen, K. W. (2015). Impacts of comprehensive information security programs on information security culture.

Journal of Computer Information Systems, *55*(3), 11-19. https://doi.org/10.1080/08874417.2015.11645767

Cheng, F. K. (2014). *Using focus groups with outsider and insider approaches: Preparation, process, and reflections*. SAGE Publications, Ltd.

Choi, K., Cronin, S., & Correia, H. (2016). The assessment of capable guardianship measures against bullying victimization in the school environment. *Police Practice and Research*, *17*(2), 149-159. https://doi.org/10.1080/15614263.2015.1128161

Choi, K. S., & Lee, J. R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. *Computers in Human Behavior*, *73*, 394–402. https://doi.org/10.1016/j.chb.2017.03.061

Chowdhury, N. H., Adam, M. T., & Teubner, T. (2020). Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. *Computers & Security*, *97*, 101931. https://doi.org/10.1016/j.cose.2020.101931

Clarke, R. V., & Felson, M. (1993). Routine activity and rational choice: Advances in criminological theory (Volume 5). *Piscataway, NJ: Transaction*. http://www.ncjrs.gov

Clarke, R. V. G. & Webb, B. (1999). *Hot products: Understanding, anticipating and reducing demand for stolen goods* (Vol. 112). London: Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate.

Clayton, P. D. (2001). Confidentiality and medical information. *Annals of emergency medicine*, *38*(3), 312-316. https://doi.org/10.1067/mem.2001.117945

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

Cohen, L. E., & Felson, M. (1979b). On estimating the social costs of national economic policy: A critical examination of the Brenner study. *Social indicators research*, 251-259. https://www.jstor.org

Coopers, P. W. (2017). Global state of information security® survey. https://www.pwc.com/gx/en/issues.html

Cornish, D. B., & Clarke, R. V. (2008). The rational choice perspective. *Environmental criminology and crime analysis*, *21*, 21-47. https://doi.org/10.4324/9780429496592

Coronado, A. J., & Wong, T. L. (2014). Healthcare cybersecurity risk management: Keys to an effective plan. *Biomedical instrumentation & technology*, *48*(s1), 26-30 https://doi.org/10.2345/0899-8205-48.s1.26

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*. https://doi.org/10.1016/j.maturitas.2018.04.008

Cronin, C. (2014). Using case study research as a rigorous form of inquiry. *Nurse researcher*, *21*(5). https://doi.org/10.7748/nr.21.5.19.e1240

Crossman, A. (2020). Understanding purposive sampling: An overview of the method and its application. https://thoughtco.com

Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A., & Sheikh, A. (2011). The case study approach. *BMC Medical Research Methodology, 11*, 100-108. https://doi.org/10.1186/1471-2288-11-100

Cruz, E. V., & Higginbottom, G. (2013). The use of focused ethnography in nursing research. *Nurse researcher*, *20*(4). https://doi.org/10.7748/nr2013.03.20.4.36.e305

Cugini, M. (2015). Successfully navigating the human subjects approval process. *Journal of Dental Hygiene*. 89(1), 54-56. https://jdh.adha.org/

Cypress, B. S. (2017). Rigor or reliability and validity in qualitative research: Perspectives, strategies, reconceptualization, and recommendations. *Dimensions of Critical Care Nursing*, *36*(4), 253-263. https://doi.org/10.1097/DCC.0000000000000253

Dameff, C., Pfeffer, M. A., & Longhurst, C. A. (2019). Cybersecurity implications for hospital quality. *Health services research*, *54*(5), 969. https://doi.org/10.1111/1475-6773.13202

de Bekker-Grob, E. W., Donkers, B., Jonker, M. F., & Stolk, E. A. (2015). Sample size requirements for discrete-choice experiments in healthcare: a practical guide. *The Patient-Patient-Centered Outcomes Research*, *8*(5), 373-384. https://doi.org/10.1007/s40271-015-0118-z

Degarmo, M. (2011). Understanding the Comparisons of Routine Activities and Contagious Distributions of Victimization: Forming a Mixed Model of Confluence and Transmission". *International Journal of Criminology and Sociological Theory*, *4*(1), 584-603. https://ijcst.journals.yorku.ca/index.php/ijcst

Demarzo, M. M. P., Cebolla, A., & Garcia-Campayo, J. (2015). The implementation of mindfulness in healthcare systems: a theoretical analysis. *General hospital psychiatry*, *37*(2), 166-171. https://doi.org/10.1016/j.genhosppsych.2014.11.013

Densham, B. (2015). Three cyber-security strategies to mitigate the impact of a data breach. *Network Security*, *2015*(1), 5–8. https://doi.org/10.1016/s1353-4858(15)70007-3

Denzin, N. K. (1978). The research act: a theoretical introduction to sociological methods. https://doi.org/10.4324/9781315134543

Dora, M., Kumar, M., & Gellynck, X. (2016). Determinants and barriers to lean implementation in food-processing SMEs–a multiple case analysis. *Production Planning & Control*, *27*(1), 1-23. https://doi.org/10.1080/09537287.2015.1050477

Dusick, D. M. (2015). BOLD Educational software: Writing the assumptions and limitations. http://www.bold-ed.com/

Eck, J. E. (1994). *Drug markets and drug places: A case-control study of the spatial structure of illicit drug dealing*. Unpublished Ph.D dissertation, College Park, MD: University of Maryland.

Eck, J., & Weisburd, D. L. (2015). Crime places in crime theory. *Crime and place: Crime prevention studies*, *4*. https://ssrn.com/abstract=2629856

Eck, J. E., & Weisburd, D. (Eds.). (1995). *Crime and place* (Vol. 4). Criminal Justice Press. https://openlibrary.org/publishers/Criminal_Justice_Press

Eichelberg, M., Kleber, K., & Kämmerer, M. (2020). Cybersecurity in PACS and medical imaging: an overview. *Journal Imaging*, *of Digital 33*(6), 1527-1542. https://doi.org/10.1007/s10278-020-00393-3

Eldefrawy, M. H., Khan, M. K., Alghathbar, K., Kim, T. H., & Elkamchouchi, H. (2012). Mobile one-time passwords: two-factor authentication using mobile phones. *Security and Communication Networks*, *5*(5), 508-516. https://doi.org/10.1002/sec.340

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of advanced research*, *5*(4), 491-497. https://doi.org/10.1016/j.jare.2014.02.006

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative content analysis: A focus on trustworthiness. *SAGE open*, *4*(1), https://doi.org/10.1177/2158244014522633

Erlingsson, C., & Brysiewicz, P. (2013). Orientation among multiple truths: An introduction of qualitative research. *African Journal of Emergency Medicine*, *3*(2), 92-99. https://doi.org/10.1016/j.afjem.2012.04.005

Erlingsson, C., & Brysiewicz, P. (2017). A hands-on guide to doing content analysis. *African Journal of Emergency Medicine*, *7*(3), 93-99. https://doi.org/10.1016/j.afjem.2017.08.001

Esteves, J., Ramalho, E., & De Haro, G. (2017). To Improve Cybersecurity, Think Like a Hacker. *MIT Sloan Management Review; Cambridge*. https://doi.org/10.1016/j.semarthrit.2004.04.002

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American journal of theoretical and applied statistics*, *5*(1), 1-4. https://doi.org/10.11648/j.ajtas.20160501.11

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks*, *9*(17), 4667-4679. https://doi.org/10.1002/sec.1657

Everett, J., Neu, D., Rahaman, A. S., & Maharaj, G. (2015). Praxis, doxa and research methods: Reconsidering critical accounting. *Critical Perspectives on Accounting, 32, 37-44.* https://doi.org/10.1016/j.cpa.2015.04.004

Farrelly, P. (2012). Selecting a research method and designing the study. *British Journal of School Nursing*, *7*, 508-511. https://doi.org/10.12968/bjsn.2012.7.10.508

Felson, M. (1995). Those who discourage crime. *Crime and place*, *4*, 53-66. https://ncjrs.gov

Felson, M., & Boba, R. L. (Eds.). (2010). *Crime and everyday life*. Sage. https://doi.org/10.4135/9781483349299

Felson, M., & Clarke, R. V. (1998). Opportunity makes the thief: Practical theory for crime prevention, *Police research series*, paper, 98. London: Home Office.

Felson, M., & Cohen, L. E. (1980). Human ecology and crime: A routine activity approach. *Human Ecology*, *8*(4), 389-406. https://doi.org/10.1007/bf01561001

Foss, N. J., & Hallberg, N. L. (2014). How symmetrical assumptions advance strategic management research. Strategic Management Journal, 35, 903-913. https://doi.org/10.1002/smj.2130

Frels, R. K., & Onwuegbuzie, A. J. (2013). Administering quantitative instruments with qualitative interviews: A mixed research approach. *Journal of Counseling & Development*, *91*(2), 184-194. https://doi.org/10.1002/j.1556-6676.2013.00085.x

Fu, K. (2011). Trustworthy medical device software. *Public Health Effectiveness of the FDA*, *510*, 102. http://css.csail.mit.edu/

Furnell, S., & Vasileiou, I. (2017). Security education and awareness: just let them burn?. *Network Security*, *2017*(12), 5-9. https://doi.org/10.1016/S1353-4858(17)30122-8

Fusch, P., Fusch, G. E., & Ness, L. R. (2018). Denzin's paradigm shift: Revisiting triangulation in qualitative research. *Journal of Social Change*, *10*(1), 2. https://doi.org/10.5590/JOSC.2018.10.1.02

Fusch, P., & Ness, L. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, *20*, 1408-1416. https://doi.org/10.46743/2160-3715/2015.2281

Galvin, R. (2015). How many interviews are enough? Do qualitative interviews in building energy consumption research produce reliable knowledge? *Journal of Building Engineering*, *1*, 2-12. https://doi.org/10.1016/j.jobe.2014.12.001

Garland, M. (1999). Multiresolution modeling: Survey & future opportunities. *State of the art report*, 111-131. http://mgarland.org/papers/

Gentles, S. J., Charles, C., Ploeg, J., & McKibbon, K. (2015). Sampling in qualitative research: Insights from an overview of the methods literature. *The Qualitative Report*, *20*(11), 1772-1789. https://doi.org/10.1016/j.exger.2006.09.013

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems*, *62*(3), 452-462. https://doi.org/10.1080/08874417.2020.1845583

Ghooi, R. B. (2014). Institutional review boards: Challenges and opportunities. *Perspectives in Clinical Research*, *5*, 60-65. https://doi.org/10.4103/2229-3485.128020

Gibson, S., Benson, O., & Brand, S. L. (2013). Talking about suicide: Confidentiality and anonymity in qualitative research. *Nursing Ethics*, *20*(1), 18-29. https://doi.org/10.1177/0969733012452684

Gill, M. J. (2014). The possibilities of phenomenology for organizational research. *Organizational research methods*, *17*(2), 118-137. https://doi.org/10.1177/1094428113518348

Gordon, W. J., Fairhall, A., & Landman, A. (2017). Threats to information security—Public health implications. *New England Journal of Medicine*, *377*(8), 707-709. https://doi.org/10.1056/NEJMp1707212

Gottfredson, M. H., & Hirschi, T. T. (1990). A general theory of crime. Stanford University Press. https://doi.org/10.1515/9781503621794

Grenier, R. S., & Dudzinska-Przesmitzki, D. (2015). A conceptual model for eliciting mental models using a composite methodology. *Human Resource Development Review*, *14*(2), 163-184. https://doi.org/10.1177/1534484315575966

Groff, E. R. (2007). Simulation for theory testing and experimentation: An example using routine activity theory and street robbery. *Journal of Quantitative Criminology*, *23*(2), 75-103. https://doi.org/10.1007/s10940-006-9021-z

Grossoehme, D. H. (2014). Overview of qualitative research. *Journal of health care chaplaincy*, *20*(3), 109-122. https://doi.org/10.1080/08854726.2014.925660

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field methods*, *18*(1), 59-82. https://doi.org/10.1177/1525822X05279903

Haegele, J. A., & Hodge, S. R. (2015). Quantitative methodology: A guide for emerging physical education and adapted physical education researchers. *The Physical Educator*, *72*(5). https://doi.org/10.18666/TPE-2015-V72-I5-6133

Hanson, J. L., Balmer, D. F., & Giardino, A. P. (2011). Qualitative research methods for medical educators. *Academic Pediatrics*, *11*, 375-386. https://doi.org/10.1016/j.acap.2011.05.001

Haraty, R. A., Kaddoura, S., & Zekri, A. S. (2018). Recovery of business intelligence systems: Towards guaranteed continuity of patient centric healthcare systems through a matrix-based recovery approach. *Telematics and Informatics*, *35*(4), 801-814. https://doi.org/10.1016/j.tele.2017.12.010

Harper, M., & Cole, P. (2012). Member checking: Can benefits be gained similar to group therapy. *The qualitative report*, *17*(2), 510-517. https://doi.org/10.46743/2160-3715/2012.2139

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. *Computers & Security*, *95*, 101827.https://doi.org/10.1016/j.cose.2020.101827

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. https://doi.org/10.1080/02732173.2017.1334608

Hawley, A. H. (1950). Human ecology: a theory of community structure. *American Sociological Review, 15*, 684. https://doi.org/10.2307/2086931

He, Y., & Johnson, C. (2015). Improving the redistribution of the security lessons in healthcare: An evaluation of the generic security template. *International Journal of Medical Informatics*. https://doi.org/10.1016/j.ijmedinf.2015.08.010

Hewig, J., Kretschmer, N., Trippe, R. H., Hecht, H., Coles, M. G. H., Holroyd, C. B., & Miltner, W. H. R. (2011). Why humans deviate from rational choice. *Psychophysiology*, *48*(4), 507–514. https://doi.org/10.1111/j.1469-8986.2010.01081.x

Hirschi, T. (1969). A control theory of delinquency. *Criminology theory: Selected classic readings*, *1969*, 289-305. https://doi.org/10.4324/9781315131511-7

Hirschi, T., & Gottfredson, M. R. (2008). 15 Critiquing the critics: The authors respond. *Out of control: Assessing the general theory of crime*, 217-231. https://doi.org/10.1515/9780804779678-017

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

Hollis-Peel, M. E., Reynald, D. M., Van Bavel, M., Elffers, H., & Welsh, B. C. (2011). Guardianship for crime prevention: A critical review of the literature. *Crime, law and social change*, *56*(1), 53-70. https://doi.org/10.1007/s10611-011-9309-2

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2018). Assessing the macro-level correlates of malware infections using a routine activities framework. *International journal of offender therapy and comparative criminology*, *62*(6), 1720-1741. https://doi.org/10.1177/0306624X16679162

Homans, G. C. (1974). Social behavior: Its elementary forms (1961). https://doi.org/10.2307/2090265

Hospital. (2016). In *Merriam-Webster.* http://www.merriam-webster.com/dictionary/hospital

Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigour in qualitative case-study research. *Nurse researcher*, *20*(4). https://doi.org/10.7748/nr2013.03.20.4.12.e326

Hu, S., Hsu, C., & Zhou, Z. (2021). Security education, training, and awareness programs: Literature review. *Journal of Computer Information Systems*, 1-13. https://doi.org/10.1080/08874417.2021.1913671

Hyett, N., Kenny, A., & Dickson-Swift, V. (2014). Methodology or method? A critical review of qualitative case study reports. *International journal of qualitative*

studies on health and well-being, *9*(1), 23606. https://doi.org/10.3402/qhw.v9.23606

Ibrahim, A., Valli, C., McAteer, I., & Chaudhry, J. (2018). A security review of local government using NIST CSF: a case study. *The Journal of Supercomputing*, *74*(10), 5171-5186. https://doi.org/10.1007/s11227-018-2479-2

Islam, S. H., Khan, M. K., & Li, X. (2015). Security analysis and improvement of 'a more secure anonymous user authentication scheme for the integrated EPR information system'. *PloS one*, *10*(8), e0131368. https://doi.org/10.1371/journal.pone.0131368

Jacob, S. A., & Furgerson, S. (2012). Writing interview protocols and conducting interviews: Tips for students new to the field of qualitative research. *Qualitative Report, 17*, 1-10. https://doi.org/10.46743/2160-3715/2012.1718

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *Journal of medical Internet research*, *20*(5). https://doi.org/10.2196/10059

Jarrett, M. P. (2017). Cybersecurity—A serious patient care concern. *JAMA*. https://doi.org/10.1001/jama.2017.11986

Johnson, S. D., & Groff, E. R. (2014). Strengthening theoretical testing in criminology using agent-based modeling. *Journal of research in crime and delinquency*, *51*(4), 509-525. https://doi.org/10.1177/0022427814531490

Jouini, M., & Rabai, L. B. A. (2016). Comparative study of information security risk assessment models for cloud computing systems. *Procedia Computer Science*, *83*, 1084-1089. https://doi.org/10.1016/j.procs.2016.04.227

Joyce, M. (2015). Using narrative in nursing research. *Nursing Standard*, *29*(38), 36-41. https://doi.org/10.7748/ns.29.38.36.e9008

Kallio, H., Pietila, A. M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing, 72*(12), 2954-2965. https://doi.org/10.1111/jan.13031

Karunarathne, S. M., Saxena, N., & Khan, M. K. (2021). Security and privacy in IoT smart healthcare. *IEEE Internet Computing*, *25*(4), 37-48 https://doi.org/10.1109/MIC.2021.3051675

Kelling, G. L., Pate, T., Dieckman, D., & Brown, C. (1974). *The Kansas City Preventive Patrol Experiment: A Technical Report*. Police Foundation. https://www.ncjrs.gov

Kennedy, W., & Olmsted, A. (2017). Three factor authentication. In *Internet Technology and Secured Transactions (ICITST), 2017 12th International Conference for* (pp. 212-213). IEEE. https://doi.org/10.23919/ICITST.2017.8356384

Ketokivi, M., & Choi, T. (2014). Renaissance of case research as a scientific method. *Journal of Operations Management*, *32*(5), 232-240. https://doi.org/10.1016/j.jom.2014.03.004

Khalind, O. S. (2019). Steganography-based Password Management: A conceptual Model. *Zanco Journal of Pure and Applied Sciences*, *31*(s3), 61-68 https://doi.org/10.1063/5.0080658

Kharraz, A., Robertson, W., & Kirda, E. (2018). Protecting against ransomware: A new line of research or restating classic ideas? *IEEE Security and Privacy*. https://doi.org/10.1109/MSP.2018.2701165

Khera, M. (2017). Think like a hacker: Insights on the latest attack vectors (and security controls) for medical device applications. *Journal of diabetes science and technology*, *11*(2), 207-212. https://doi.org/10.1177/1932296816677576

Khey, D. N., & Sainato, V. A. (2013). Examining the correlates and spatial distribution of organizational data breaches in the United States. *Security Journal, 26*, 367-382. https://doi.org/10.1057/sj.2013.24

Khoumsi, A., Erradi, M., & Krombi, W. (2018). A formal basis for the design and analysis of firewall security policies. *Journal of King Saud University-Computer and Information Sciences*, *30*(1), 51-66. https://doi.org/10.1016/j.jksuci.2016.11.008

Kihn, L. A., & Ihantola, E. M. (2015). Approaches to validation and evaluation in qualitative studies of management accounting. *Qualitative Research in Accounting & Management*, *12*(3), 230-255. https://doi.org/10.1108/QRAM-03-2013-0012

Kim, D. W., Choi, J. Y., & Han, K. H. (2020). Medical device safety management using cybersecurity risk analysis. *IEEE Access*, *8*, 115370-115382. https://doi.org/10.1109/ACCESS.2020.3003032

Kim, L. (2018). Cybersecurity matters. *Nursing management*, *49*(2), 16-22. https://doi.org/10.1097/01.numa.0000529921.97762.be

Kipkulei, K. (2013). *Effects of information technology on reducing perishable waste in supermarkets* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 3560427)

Klokman, V. W., Barten, D. G., Peters, N. A., Versteegen, M. G., Wijnands, J. J., van Osch, F. H., Gaakeer, M. I., Tan, E. C., & Boin, A. (2021). A scoping review of internal hospital crises and disasters in the Netherlands, 2000–2020. *PloS one*, *16*(4), e0250551. https://doi.org/10.1371/journal.pone.0250551

Klonoff, D. C. (2015). Cybersecurity for connected diabetes devices. *Journal of Diabetes Science and Technology*. https://doi.org/10.1177/1932296815583334

Koc, E., & Boz, H. (2014). Triangulation in tourism research: A bibliometric study of top three tourism journals. *Tourism Management Perspectives*, *12*, 9-14. https://doi.org/10.1016/j.ijcip.2015.02.002

Kogetsu, A., Ogishima, S., & Kato, K. (2018). Authentication of patients and participants in health information exchange and consent for medical research: A key step for privacy protection, respect for autonomy, and Trustworthiness. *Frontiers in Genetics*. https://doi.org/10.3389/fgene.2018.00167

Kornbluh, M. (2015). Combatting challenges to establishing trustworthiness in qualitative research. *Qualitative research in psychology*, *12*(4), 397-414. https://doi.org/10.1080/14780887.2015.1021941

Krisberg, K. (2017). Cybersecurity: Public health increasingly facing threats. *American Journal of Public Health*, *107*(8), 1195. http://ajph.aphapublications.org

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1-10. https://doi.org/10.3233/THC-161263.

Kyvik, S. (2013). The academic researcher role: Enhancing expectations and improved performance. *Higher Education*, *65*, 525-538. https://doi.org/10.1007/s10734-012-9561-0

Lawlor, D. A., Tilling, K., & Davey Smith, G. (2016). Triangulation in aetiological epidemiology. *International Journal of Epidemiology*, *45*(6), 1866-1886. https://doi.org/10.1093/ije/dyw314

Lee, J., de Guzman, M. C., Talebi, N., Korni, S. K., Szumigala, D., & Rao, H. R. (2018). Use of online information and suitability of target in shoplifting: A routine activity based analysis. *Decision Support Systems*, *110*, 1-10. https://doi.org/10.1016/j.dss.2018.03.001

Leech, N. L., & Onwuegbuzie, A. J. (2007). An array of qualitative data analysis tools: A call for data analysis triangulation. *School Psychology Quarterly*, *22*, 557-584. https://doi.org/10.1037/1045-3830.22.4.557

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

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of family medicine and primary care*, *4*(3), 324. https://doi.org/10.4103/2249-4863.161306

Li, C. T., Weng, C. Y., & Lee, C. C. (2015). A secure RFID tag authentication protocol with privacy preserving in telecare medicine information system. *Journal of Medical Systems*. https://doi.org/10.1007/s10916-015-0260-0

Li, X., Niu, J., Karuppiah, M., Kumari, S., & Wu, F. (2016). Secure and efficient two-factor user authentication scheme with user anonymity for network based e-Health care applications. *Journal of Medical Systems*. https://doi.org/10.1007/s10916-016-0629-8

Lim, S. S., Vos, T., Flaxman, A. D., Danaei, G., Shibuya, K., Adair-Rohani, H., AlMazroa, M. A., Amann, M., Anderson, H. R., Andrews, K. G., & Aryee, M. (2012). A comparative risk assessment of burden of disease and injury attributable to 67 risk factors and risk factor clusters in 21 regions, 1990–2010: a systematic analysis for the Global Burden of Disease Study 2010. *The lancet*, *380*(9859), 2224-2260. https://doi.org/10.1016/s0140-6736(12)61766-8

Liu, Y., He, D., Obaidat, M. S., Kumar, N., Khan, M. K., & Choo, K. K. R. (2020). Blockchain-based identity management systems: A review. *Journal of network*

and computer applications, *166*, 102731. https://doi.org/10.1016/j.jnca.2020.102731

Lo Iacono, V., Symonds, P., & Brown, D. H. (2016). Skype as a tool for qualitative research interviews.*Sociological Research Online*, *21*(2), 1-15. https://doi.org/10.5153/sro.3952

Lošonczi, P., Nečas, P., & Naď, N. (2016). Risk management in information security. *Journal of Management*, (1), 28,

Lowry, P. B., Posey, C., Bennett, R. B. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal*, *25*(3), 193-273. https://doi.org/10.1111/isj.12063

Malterud, K., Siersma, V. D., & Guassora, A. D. (2016). Sample size in qualitative interview studies: guided by information power. *Qualitative health research*, *26*(13), 1753-1760. https://doi.org/10.1177/1049732315617444

Mansfield, E., Sowards, J. W., & Crookes-Goodson, W. J. (2015). Findings and recommendations from the NIST Workshop on alternative fuels and materials: biocorrosion. *Journal of research of the National Institute of Standards and Technology*, *120*, 28. https://doi.org/10.6028/jres.120.003

Mansfield-Devine, S. (2016). Ransomware: taking businesses hostage. *Network Security*. https://doi.org/10.1016/S1353-4858(16)30096-4

Mansfield-Devine, S. (2017). Leaks and ransoms – the key threats to healthcare organisations. *Network Security*. https://doi.org/10.1016/S1353-4858(17)30062-4

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons*, *59*(3), 257-266 https://doi.org/10.1016/j.bushor.2016.01.002

Marshall, M. N. (1996). Sampling for qualitative research. Family Practice, 13(6), 522-526. https://doi.org/10.1093/fampra/13.6.522

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? *BMJ (Online)*, *358*. https://doi.org/10.1136/bmj.j3179

Massey, J. L., Krohn, M. D., & Bonati, L. M. (1989). Property crime and the routine activities of individuals. *Journal of Research in Crime and Delinquency*, *26*(4), 378-400. https://doi.org/10.1177/0022427889026004004

Mayhew, P., Clarke, R. V., Sturman, A., & Hough, J. M. (1976). Home Office Research Study No. 34. *Crime as Opportunity*, 9-20. https://www.ojp.gov/ncjrs/virtual-library/abstracts/crime-opportunity

McCusker, K., & Gunaydin, S. (2015). Research using qualitative, quantitative or mixed methods and choice based on the research. *Perfusion*, *30*(7), 537-542. https://doi.org/10.1177/0267659114559116

McFadyen, J., & Rankin, J. (2016). The role of gatekeepers in research: learning from reflexivity and reflection. *GSTF Journal of Nursing and Health Care*, *4*(1), 82-88. https://doi.org/10.5176/2345-718X_4.1.135

McGuire, C. F. (2015). TIM lecture series-The expanding cybersecurity threat. *Technology Innovation Management Review*, *5*(3), 56. https://doi.org/10.22215/timreview/881

McNeeley, S. (2015). Lifestyle-routine activities and crime events. *Journal of Contemporary Criminal Justice*, *31*(1), 30-52. https://doi.org/10.1177/1043986214552607

Miao, L., & Li, S. (2017). Cyber security based on mean field game model of the defender: Attacker strategies. *International Journal of Distributed Sensor Networks*, *13*(10). https://doi.org/10.1177/1550147717737908

Miró, F. (2014). Routine activity theory. *The encyclopedia of theoretical criminology*, 1-7. https://doi.org/10.1002/9781118517390.wbetc198

Mohammed, D. (2017). US Healthcare Industry: Cybersecurity Regulatory and Compliance Issues. *Journal of Research in Business, Economics and Management*, *9*(5), 1771-1776. https://doi.org/10.48009/1_iis_2021_10-50

Mohammed, D., Mariani, R., & Mohammed, S. (2015). Cybersecurity challenges and compliance issues within the US healthcare sector. *International Journal of Business and Social Research*, *5*(2), 55-66. https://doi.org/10.18533/ijbsr.v5i2.714

Morgan, S. (Ed.), (2017). Ransomware damage report. *Cybersecurity Ventures.* https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/

Morse, J. M. (2015). Critical analysis of strategies for determining rigor in qualitative inquiry. *Qualitative health research*, *25*(9), 1212-1222. https://doi.org/10.1177/1049732315588501

Moses, V., & Korah, I. (2015). Lack of security of networked medical equipment in radiology. *American Journal of Roentgenology*, *204*(2), 343-353. https://doi.org/10.2214/AJR.14.12882

Moustakas, C. (1994). *Phenomenological research methods.* Sage Publications Inc.

Munn, Z., Porritt, K., Lockwood, C., Aromataris, E., & Pearson, A. (2014). Establishing confidence in the output of qualitative research synthesis: the ConQual approach. *BMC medical research methodology*, *14*(1), 108. https://doi.org/10.1186/1471-2288-14-108

Murray, J. S. (1999). Methodological triangulation in a study of social support for siblings of children with cancer. *Journal of Pediatric Oncology Nursing*, *16*(4), 194-200. https://doi.org/10.1016/S1043-4542(99)90019-X

Murthy, D. (2013). Ethnographic Research 2.0: The potentialities of emergent digital technologies for qualitative organizational research. *Journal of Organizational Ethnography*, *2*(1), 23-36. https://doi.org/10.1108/JOE-01-2012-0008

Mustaine, E. E., & Tewksbury, R. (2000). Comparing the lifestyles of victims, offenders, and victim-offenders: A routine activity theory assessment of similarities and differences for criminal incident participants. *Sociological Focus*, *33*(3), 339-362. https://doi.org/10.1080/00380237.2000.10571174

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. In *Forum: Qualitative Social Research* (Vol. 19, No. 3, pp. 783-797). Freie Universität Berlin.

Naseer, H., Maynard, S. B., & Desouza, K. C. (2021). Demystifying analytical information processing capability: The case of cybersecurity incident response. *Decision Support Systems*, *143*, 113476. https://doi.org/10.1016/j.dss.2020.113476

Navarro, J. N., & Jasinski, J. L. (2012). Going cyber: Using routine activities theory to predict cyberbullying experiences. *Sociological Spectrum*, *32*(1), 81-94. https://doi.org/10.1080/02732173.2012.628560

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence-based nursing*, *18*(2), 34-35. https://doi.org/10.1136/eb-2015-102054

Offner, K. L., Sitnikova, E., Joiner, K., & MacIntyre, C. R. (2020). Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation. *Intelligence and National Security*, *35*(4), 556-585. https://doi.org/10.1080/02684527.2020.1752459

Onwuegbuzie, A. J., & Corrigan, J. A. (2014). Improving the quality of mixed research reports in the field of human resource development and beyond: A call for rigor as an ethical practice. *Human Resource Development Quarterly,* 25(3), 273-299. https://doi.org/10.1002/hrdq.21197

Osgood, D. W., Wilson, J. K., O'malley, P. M., Bachman, J. G., & Johnston, L. D. (1996). Routine activities and individual deviant behavior. *American Sociological Review*, 635-655. https://doi.org/10.2307/2096397

Ozair, F. F., Jamshed, N., Sharma, A., & Aggarwal, P. (2015). Ethical issues in electronic health records: A general overview. *Perspectives in clinical research*, *6*(2), 73. https://doi.org/10.4103/2229-3485.153997

Pack, M. (2014). Practice journeys: using online reflective journals in social work fieldwork education, *Reflective Practice*, 15:3, 404-412. https://doi.org/10.1080/14623943.2014.883304

Palinkas, L. A., Fuentes, D., Finno, M., Garcia, A. R., Holloway, I. W., & Chamberlain, P. (2014). Inter-organizational collaboration in the implementation of evidence-based practices among public agencies serving abused and neglected youth. *Administration and Policy in Mental Health and Mental Health Services Research*, *41*(1), 74-85. https://doi.org/10.1007/s10488-012-0437-5

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and policy in mental health and mental health services research*, *42*(5), 533-544. https://doi.org/10.1007/s10488-013-0528-y

Paternoster, R., Bachman, R., Bushway, S., Kerrison, E., & O'Connell, D. (2015). Human agency and explanations of criminal desistance: Arguments for a rational choice theory. *Journal of Developmental and Life-Course Criminology*, *1*(3), 209-235. https://doi.org/10.1007/s40865-015-0013-2

Patton, M. Q. (1999). Enhancing the quality and credibility of qualitative analysis. *Health services research*, *34*(5 Pt 2), 1189. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1089059/

Paulus, T. M., & Bennett, A. M. (2017). 'I have a love–hate relationship with ATLAS. ti'™: integrating qualitative data analysis software into a graduate research methods course. *International Journal of Research & Method in Education*, *40*(1), 19-35. https://doi.org/10.1080/1743727X.2015.1056137

Perakslis, E. D., & Stanley, M. (2016). A cybersecurity primer for translational research. *Science translational medicine*, *8*(322), 322ps2-322ps2. https://doi.org/10.1126/scitranslmed.aaa4493

Peters, K., & Halcomb, E. (2015). Interviews in qualitative research. *Nurse Researcher (2014+)*, *22*(4), 6. https://doi.org/10.7748/nr.22.4.6.s2

Peticca-Harris, A., deGama, N., & Elias, S. R. (2016). A dynamic process model for finding informants and gaining access in qualitative research. *Organizational Research Methods*, *19*(3), 376-401. https://doi.org/10.1177/1094428116629218

Petty, N. J., Thomson, O. P., & Stew, G. (2012). Ready for a paradigm shift? Part 2: Introducing qualitative research methodologies and methods. *Manual Therapy*, *17*, 378-384. https://doi.org/10.1016/j.math.2012.03.004

Pezalla, A. E., Pettigrew, J., & Miller-Day, M. (2012). Researching the researcher-as-instrument: An exercise in interviewer self-reflexivity. *Qualitative Research*, *12*, 165-185. https://doi.org/10.1177/1468794111422107

Pigni, F., Bartosiak, M., Piccoli, G., & Ives, B. (2018). Targeting Target with a 100 million dollar data breach. *Journal of Information Technology Teaching Cases*. https://doi.org/10.1057/s41266-017-0028-0

Pratt, T. C., & Turanovic, J. J. (2016). Lifestyle and routine activity theories revisited: The importance of "risk" to the study of victimization. *Victims & Offenders*, *11*(3), 335-354. https://doi.org/10.1080/15564886.2015.1057351

Pugh, J., Pycroft, L., Sandberg, A., Aziz, T., & Savulescu, J. (2018). Brainjacking in deep brain stimulation and autonomy. *Ethics and Information Technology*, 1-14. https://doi.org/10.1007/s10676-018-9466-4

Purohit, B., & Singh, P. P. (2013). Data leakage analysis on cloud computing. *International Journal of Engineering Research and Applications*, *3*(3), 1311-1316. https://www.ijera.com

Pycroft, L., Boccard, S. G., Owen, S. L. F., Stein, J. F., Fitzgerald, J. J., Green, A. L., & Aziz, T. Z. (2016). Brainjacking: Implant security issues in invasive neuromodulation. *World Neurosurgery*. https://doi.org/10.1016/j.wneu.2016.05.010

Pyrooz, D. C., Decker, S. H., & Moule, R. K., Jr. (2015). Criminal and routine activities in online settings: Gangs, offenders, and the Internet. *Justice Quarterly*, *32*(3), 471-499. https://doi.org/10.1080/07418825.2013.778326

Raeburn, T., Schmied, V., Hungerford, C., & Cleary, M. (2015). The contribution of case study design to supporting research on clubhouse psychosocial rehabilitation. *BMC research notes*, *8*(1), 521. https://doi.org/10.1186/s13104-015-1521-1

Ranney, M. L., Meisel, Z. F., Choo, E. K., Garro, A. C., Sasson, C., & Morrow Guthrie, K. (2015). Interview-based qualitative research in emergency care part II: Data collection, analysis and results reporting. *Academic Emergency Medicine*, *22*(9), 1103-1112. https://doi.org/10.1111/acem.12735

Rapp, S. R., Legault, C., Espeland, M. A., Resnick, S. M., Hogan, P. E., Coker, L. H., Dailey, M., Shumaker, S. A., & The CAT Study Group, (2012). Validation of a cognitive assessment battery administered over the telephone. *Journal of the American Geriatrics Society*, *60*(9), pp.1616-1623. https://doi.org/10.1111/j.1532-5415.2012.04111.x

Rathi, A., & Parmar, N. (2015). Secure cloud data computing with third party auditor control. *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014*, 145–152. https://doi.org/10.1007/978-3-319-12012-6_17

Reyns, B. W. (2015). A routine activity perspective on online victimisation: Results from the Canadian General Social Survey. *Journal of Financial Crime*, *22*(4), 396-411. https://doi.org/10.1108/JFC-06-2014-0030

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International journal of offender therapy and comparative criminology*, *60*(10), 1119-1139. https://doi.org/10.1177/0306624X15572861

Reyns, B. W., & Scherer, H. (2019). Disability Type and Risk of Sexual and Stalking Victimization in a National Sample: A Lifestyle–Routine Activity Approach.

Criminal Justice and Behavior, *46*(4), 628-647. https://doi.org/10.1177/0093854818809148

Richardson, R., & North, M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, *13*(1), 10-21. http://www.imrjournal.org/

Rios, B. (2015). Cybersecurity expert: medical devices have 'a long way to go'. *Biomedical instrumentation & technology*, *49*(3), 197-200. https://doi.org/10.2345/0899-8205-49.3.197

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, *2*(2), 121-135. https://doi.org/10.1093/cybsec/tyw001

Rubin, H. J., & Rubin, I. S. (2011). *Qualitative interviewing: The art of hearing data* (3rd ed.). Sage.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65-78. https://doi.org/10.1016/j.cose.2015.05.012

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70-82. https://doi.org/10.1016/j.cose.2015.10.006

Sampson, R., Eck, J. E., & Dunham, J. (2010). Super controllers and crime prevention: A routine activity explanation of crime prevention success and failure. *Security Journal*, *23*(1), 37-51. https://doi.org/10.1057/sj.2009.17

Samtani, S., Chai, Y., & Chen, H. (2022). Linking exploits from the dark web to known vulnerabilities for proactive cyber threat intelligence: An attention-based deep

structured semantic model. *MIS Quarterly*, *46*(2), 911-946. https://doi.org/10.25300/MISQ/2022/15392

Sani, A. S., Yuan, D., Jin, J., Gao, L., Yu, S., & Dong, Z. Y. (2019). Cyber security framework for Internet of Things-based Energy Internet. *Future Generation Computer Systems*, *93*, 849-859. https://doi.org/10.1016/j.future.2018.01.029

Sarma, S. K. (2015). Qualitative research: Examining the misconceptions. *South Asian Journal of Management*, *22*(3), 176.

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

Schochow, M., Schnell, D., & Steger, F. (2015). Implementation of clinical ethics consultation in German hospitals. *Science and engineering ethics*, 1-7. https://doi.org/10.1007/s11948-016-9805-y

Sebescen, N., & Vitak, J. (2017). Securing the human: Employee security vulnerability risk in organizational settings. *Journal of the Association for Information Science and Technology*, *68*(9), 2237-2247. https://doi.org/10.1002/asi.23851

Seyal, A. H. (2015). Examining the Role of Transformational Leadership in Technology Adoption: Evidence from Bruneian Technical & Vocational Establishments (TVE). *Journal of Education and Practice*, *6*(8), 32-43. https://doi.org/10.7176/JEP

Shaik, S. A., & Alowaidi, M. (2022). A Secure and Robust Architecture based on Mobile Healthcare Applications for Patient Monitoring Environments. *International*

Journal of Advanced Computer Science and Applications, *13*(2). https://doi.org/10.14569/IJACSA.2022.0130261

Shamsi, J. A., Zeadally, S., Sheikh, F., & Flowers, A. (2016). Attribution in cyberspace: techniques and legal implications: SCN-SI-088. *Security and Communication Networks*, *9*(15), 2886-2900. https://doi.org/10.1002/sec.1485

Shaw, C. R., Zorbaugh, Harvey, McKay, Henry D., & Cottrell, Leonard S. (1929). *Delinquency Areas*. Chicago: University of Chicago Press. https://doi.org/10.1037/13522-002

Shenoy, A., & Appel, J. M. (2017). Safeguarding confidentiality in electronic health records. *Cambridge Quarterly of Healthcare Ethics*, *26*(2), 337-341. https://doi.org/10.1017/S0963180116000931

Sherman, L. W., Gartin, P. R., & Buerger, M. E. (1989). Hot spots of predatory crime: Routine activities and the criminology of place. *Criminology*, *27*(1), 27-56. https://doi.org/10.1111/j.1745-9125.1989.tb00862.x

Sidhu, K., Jones, R., & Stevenson, F. (2017). Publishing qualitative research in medical journals. *British Journal of General Practice*, *67*(658), 229-230. https://doi.org/10.3399/bjgp17x690821

Sikorskii, A., & Noble, P. C. (2013). Statistical considerations in the psychometric validation of outcome measures. *Clinical Orthopaedics & Related Research®*, *471*(11), 3489-3495. https://doi.org/10.1007/s11999-013-3028-1

Singh, H., & Sittig, D. F. (2016). Measuring and improving patient safety through health information technology: The Health IT Safety Framework. *BMJ Quality & Safety*, bmjqs-2015. https://doi.org/10.1136/bmjqs-2015-004486

Singh, K. (2016). A small study on impact of crime against women news stories on Indian urban women. *Imperial Journal of Interdisciplinary Research*, *2*(3), 60-68. http://www.onlinejournal.in/ijir/

Sittig, D. F., & Singh, H. (2015). A new socio-technical model for studying health information technology in complex adaptive healthcare systems. In *Cognitive informatics for biomedicine* (pp. 59-80). Springer, Cham. https://doi.org/10.1136/qshc.2010.042085

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & security*, *57*, 14-30. https://doi.org/10.1016/j.cose.2015.11.001

Sorsa, M. A., Kiikkala, I., & Astedt-Kurki, P. (2015). Bracketing as a skill in conducting unstructured qualitative interviews. *Nurse researcher*, *22*(4). https://doi.org/10.7748/nr.22.4.8.e1317

Stake, R. E. (1995). *The art of case study research*. sage.

Stewart, J. (2012). Multiple-case study methods in governance-related research. *Public Management Review*, *14*(1), 67-82. https://doi.org/10.1080/14719037.2011.589618

Stichler, J. F. (2014). The ethics of research, writing, and publication. *Health Environments Research & Design Journal (HERD)*, *8*(1), 15-19. https://doi.org/10.1177/193758671400800103

Stine, I., Rice, M., Dunlap, S., & Pecarina, J. (2017). A cyber risk scoring system for medical devices. *International Journal of Critical Infrastructure Protection*, *19*, 32-46. https://doi.org/10.1016/j.ijcip.2017.04.001

Stobert, E., & Biddle, R. (2018). The password life cycle. *ACM Transactions on Privacy and Security (TOPS)*, *21*(3), 1-32. https://doi.org/10.1145/3183341

Stoop, E. M., de Wijkerslooth, T. R., Bossuyt, P. M., Stoker, J., Fockens, P., Kuipers, E. J., Dekker, E., & van Leerdam, M. E. (2012). Face-to-face vs telephone pre-colonoscopy consultation in colorectal cancer screening; A randomised trial. *British Journal of Cancer*, *107*, 1051-1058. https://doi.org/10.1038/bjc.2012.358

Stratton, G., Powell, A., & Cameron, R. (2017). Crime and justice in digital society: Towards a 'digital criminology'?. *International Journal for Crime, Justice and Social Democracy*, *6*(2), 17. https://doi.org/10.5204/ijcjsd.v6i2.355

Suri, H. (2011). Purposeful sampling in qualitative research synthesis. *Qualitative research journal*, *11*(2), 63. https://doi.org/10.3316/QRJ1102063

Svensson, L., & Doumas, K. (2013). Contextual and analytic qualities of research methods exemplified in research on teaching. *Qualitative inquiry*, *19*(6), 441-450. https://doi.org/10.1177/1077800413482097

Swauger, M. (2011). Afterword: The ethics of risk, power, and representation. *Qualitative Sociology*, *34*, 497-502. https://doi.org/10.1007/s11133-011-9201-5

Swede, M. J., Scovetta, V., & Eugene-Colin, M. (2019). Protecting patient data is the new scope of practice: A recommended cybersecurity curricula for healthcare students to prepare for this challenge. *Journal of Allied Health*, *48*(2), 148-156. https://www.ingentaconnect.com/content/asahp/jah/2019/00000048/00000002/art00013

Tamariz, L., Palacio, A., Robert, M., & Marcus, E. N. (2013). Improving the informed consent process for research subjects with low literacy: A systematic review. *Journal of General Internal Medicine*, *28*, 121-126. https://doi.org/10.1007/s11606-012-2133-2

Taylor, P. J., & Gunn, J. (1999). Homicides by people with mental illness: myth and reality. *The British Journal of Psychiatry*, *174*(1), 9-14. https://doi.org/10.1192/bjp.174.1.9

Tewksbury, R., & Mustaine, E. E. (2001). Lifestyle factors associated with the sexual assault of men: A routine activity theory analysis. *The Journal of Men's Studies*, *9*(2), 153-182. https://doi.org/10.3149/jms.0902.153

Thaduri, A., Aljumaili, M., Kour, R., & Karim, R. (2019). Cybersecurity for eMaintenance in railway infrastructure: risks and consequences. *International Journal of System Assurance Engineering and Management*, *10*(2), 149-159. https://doi.org/10.1007/s13198-019-00778-w

Tilley, N. (2014). *Crime prevention*. Willan. https://doi.org/10.4324/9781315820071

Tillyer, M. S., & Eck, J. E. (2009). Routine activities. *21st century criminology: A reference handbook*, *1*, 279-287. https://doi.org/10.4135/9781412971997.n32

Tomkinson, S. (2014, November). Doing fieldwork on state organizations in democratic settings: Ethical issues of research in refugee decision making. In *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research* (Vol. 16, No. 1). https://doi.org/10.17169/fqs-16.1.2201

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. https://doi.org/10.1016/j.jclinepi.2016.07.014

Trier-Bieniek, A. (2012). Framing the telephone interview as a participant-centred tool for qualitative research: a methodological discussion. *Qualitative Research*, *12*(6), 630-644. https://doi.org/10.1177/1468794112439005

Tseloni, A., & Pease, K. (2015). Area and individual differences in personal crime victimization incidence: The role of individual, lifestyle/routine activities and contextual predictors. *International review of victimology*, *21*(1), 3-29. https://doi.org/10.1177/0269758014547991

Tseloni, A., Wittebrood, K., Farrell, G., & Pease, K. (2004). Burglary victimization in England and Wales, the United States and the Netherlands: A cross-national comparative test of routine activities and lifestyle theories. *British Journal of Criminology*, *44*(1), 66-91. https://doi.org/10.1093/bjc/44.1.66

Tufford, L., & Newman, P. (2012). Bracketing in qualitative research. *Qualitative Social Work*, *11*(1), 80-96. https://doi.org/10.1177/1473325010368316

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

Unluer, S. (2012). Being an insider researcher while conducting case study research. *Qualitative Report*, *17*, 58. https://doi.org/10.46743/2160-3715/2012.1752

U.S. Department of Health and Human Services, Office for Civil Rights (2015). *Breaches affecting 500 or more individuals.* https://ocrportal.hhs.gov/breach/breach_report.jsf

Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & health sciences*, *15*(3), 398-405. https://doi.org/10.1111/nhs.12048

Vakhitova, Z. I., Reynald, D. M., & Townsley, M. (2015). Toward the adaptation of routine activity and lifestyle exposure theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice*. *32*, 169–188. https://doi.org/10.1177/1043986215621379

Valenzuela, D., & Shrivastava, P. (2002). Interview as a method for qualitative research. *Southern Cross University and the Southern Cross Institute of Action Research (SCIAR)*. https://www.public.asu.edu/

van Rijnsoever, F. J. (2017). (I can't get no) saturation: A simulation and guidelines for sample sizes in qualitative research. PL o S One, 12(7), 1–17. https://doi.org/10.1371/journal.pone.0181689

Vannoni, M. (2015). What Are Case Studies Good for? Nesting Comparative Case Study Research Into the Lakatosian Research Program. *Cross-Cultural Research*. https://doi.org/10.1177/1069397114555844

Vasileiou, K., Barnett, J., Thorpe, S., & Young, T. (2018). Characterising and justifying sample size sufficiency in interview-based studies: systematic analysis of qualitative health research over a 15-year period. *BMC medical research methodology*, *18*(1), 148. https://doi.org/10.1186/s12874-018-0594-7

Veksler, V. D., Buchler, N., Hoffman, B. E., Cassenti, D. N., Sample, C., & Sugrim, S. (2018). Simulations in cyber-security: a review of cognitive modeling of network attackers, defenders, and users. *Frontiers in psychology*, *9*, 691. https://doi.org/10.3389/fpsyg.2018.00691

Wang, C. C., & Geale, S. K. (2015). The power of story: Narrative inquiry as a methodology in nursing research. *International Journal of Nursing Sciences*. https://doi.org/10.1016/j.ijnss.2015.04.014

Wang, D., He, D., Wang, P., & Chu, C. H. (2015). Anonymous Two-Factor Authentication in Distributed Systems: Certain Goals Are Beyond Attainment. *IEEE Transactions on Dependable and Secure Computing*. https://doi.org/10.1109/TDSC.2014.2355850

Wang, J., Gupta, M., & Rao, H. R. (2015). Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications. *MIS Quarterly*. https://doi.org/10.25300/MISQ/2015/39.1.05

Webb, T., & Dayal, S. (2017). Building the wall: Addressing cybersecurity risks in medical devices in the USA and Australia. *Computer Law & Security Review*, *33*(4), 559-563. https://doi.org/10.1016/j.clsr.2017.05.004

Weisburd, D., Wyckoff, L. A., Ready, J., Eck, J. E., Hinkle, J. C., & Gajewski, F. (2006). Does crime just move around the corner? A controlled study of spatial displacement and diffusion of crime control benefits. *Criminology*, *44*(3), 549-592. https://doi.org/10.1111/j.1745-9125.2006.00057.x

Welch, D., Grossaint, K., Reid, K., & Walker, C. (2014). Strengths-based leadership development: Insights from expert coaches. *Consulting Psychology Journal: Practice and Research*, *66*(1), 20. https://doi.org/10.1037/cpb0000002

Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical Devices (Auckland, NZ)*, *8*, 305. https://doi.org/10.2147/mder.s50048

Wirth, A. (2017). The economics of cybersecurity. *Biomedical instrumentation & technology*, *51*(s6), 52-59. https://doi.org/10.2345/0899-8205-51.s6.52

Wolgemuth, J. R. (2014). Analyzing for critical resistance in narrative research. *Qualitative Research*, *14*(5), 586-602. https://doi.org/10.1177/1468794113501685

Wright, A., Aaron, S., & Bates, D. W. (2016). The big phish: Cyberattacks against U.S. healthcare systems. *Journal of General Internal Medicine*. https://doi.org/10.1007/s11606-016-3741-z

Wright, B., & Ogbuehi, A. O. (2014). Surveying adolescents: The impact of data collection methodology on response quality. *Electronic Journal of Business Research Methods*, *12*(1), 41-53. http://www.ejbrm.com

Wu, F., & Eagles, S. (2016). Cybersecurity for medical device manufacturers: Ensuring safety and functionality. *Biomedical Instrumentation and Technology*. https://doi.org/10.2345/0899-8205-50.1.23

Xiong, H., Tao, J., & Chen, Y. (2016). A Robust and anonymous two factor authentication and key agreement protocol for telecare medicine information systems. *Journal of medical systems*, *40*(11), 228. https://doi.org/10.1007/s10916-016-0590-6

Xiong, H., Tao, J., & Yuan, C. (2017). Enabling telecare medical information systems with strong authentication and anonymity. *IEEE Access*. https://doi.org/10.1109/ACCESS.2017.2678104

Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2021). Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. *International Journal of Information Security*, 1-44.

Yadron, D. (2016). Los Angeles hospital paid $17,000 in bitcoin to ransomware hackers. *The Guardian*. https://www.theguardian.com

Ye, B., Khan, S. S., Chikhaoui, B., Iaboni, A., Martin, L. S., Newman, K., Wang, A., & Mihailidis, A. (2018). Challenges in Collecting Big Data in A Clinical Environment with Vulnerable Population: Lessons Learned from A Study Using

A Multi-modal Sensors Platform. *Science and Engineering Ethics*, 1-20. https://doi.org/10.1007/s11948-018-0072-y

Yin, R. K. (2013). Validity and generalization in future case study evaluations. *Evaluation*, *19*(3), 321–332. https://doi.org/10.1177/1356389013497081

Yin, R. K. (2014). *Case study research: Design and methods* (5th ed.). Sage.

Yeoh, W., & Popovič, A. (2016). Extending the understanding of critical success factors for implementing business intelligence systems. *Journal of the Association for Information Science and Technology*, *67*(1), 134-147. https://doi.org/10.1002/asi.23366

Young, D., Lopez, J., Jr., Rice, M., Ramsey, B., & McTasney, R. (2016). A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection*, *14*, 43-57. https://doi.org/10.1016/j.ijcip.2016.04.001

Yu, J., Ha, J. W., & Oh, D. Y. (2008). Causes of conflicts of local information technology manager in multinational company. *Academy of Information and Management Sciences*, *12*(1), 23. https://www.alliedacademies.org/

Zachariadis, M., Scott, S., & Barrett, M. (2013). Methodological implications of critical realism for mixed-methods research. *MIS quarterly*, 855-879. https://doi.org/10.25300/misq/2013/37.3.09

Zaharia, G. C., Zaharia, C., Tudorescu, N., & Zaharia, I. (2010). Online crime and the regulation of business on the Internet. *Economics, Management, and Financial Markets*, *5*(4), 238-243. https://addletonacademicpublishers.com/economics-

management-and-financial-markets

Zandona, D. J., & Thompson, J. M. (2017). Going beyond compliance: A strategic framework for promoting information security in hospitals. *Health Care Manager* 36(4), 364-371. https://doi.org/10.1097/HCM.0000000000000189

Zivkovic, J. (2012). Strengths and weakness of business research methodologies: Two disparate case studies. *Business Studies Journal*, *4*(2), 91-99. http://www.alliedacademies.org/business-studies-journal/

Appendix A: Letter of Cooperation From Hospitals' Company Leaders

[Hospital Leader Name]
[Title]
[Hospital Name]

Date

Dear Hospital Leader Name,

My name is Donovan Pottinger, a doctoral student at Walden University working to obtain a Doctor of Information Technology (DIT) degree with a specialization in Cybersecurity. I am conducting a doctoral study to explore the strategies to reduce cybersecurity breaches in hospitals. Donovan Pottinger's background is in information technology.

This is an invitation for your company to take part in research. Your company is of interest because you have been identified as a hospital who implement information security solutions to combat cybersecurity threats and breaches. You are receiving this email because of your position as an IT leader in an hospital that has the authority to grant permission to conduct a case study on your hospital's IT infrastructure. A requirement for company acceptance to participate in the research is for the company leader to provide email addresses and contact phone numbers for two IT security manager (research participants) at the firm. The criteria for the IT security managers are employees who have adopted cybersecurity strategies to combat cyberattacks on the hospital patients and customers' sensitive information such as Protected Health Information (PHI).

Company/Employee

- As I receive the hospital company leader's email confirmation with the IT security managers contacts, I will conduct an initial meeting to discuss the research process in more details with the IT security managers.
- I will send an email invitation including an inform consent form to the ITsecurity manager, where the companys leader granted permission to conduct the study.

Research Method

I will meet the research participants' face-to-face in person or through Skype for the first interviews to extract research data and utilize the telephone for follow-up interviews. As the IT leaders provide email confirmations with a signed informed consent form to participate in the research, I will call to introduce myself further and set up interviews. Time commitment involves two audiotaped interviews for the face-to-face and follow-up telephone interviews for an hour each. I will audiotape the interview to ensure accurate transcription of the interview data. In addition, I will require documentation (company

documents, archival records, or public information) that could help me enhance my understanding of the research.

Location of Research

The face-to-face interview will take place at a time, date, and location outside the participant's company workplace and time that aligns with their schedule. For a follow-up telephone interview, the time scheduled to conduct the interview will depend on a time suitable for the participants to provide research data.

Confidentiality

I will ensure the information the research participants provide is kept confidential. I will not utilize the information beyond the purpose of this study. The study report will not include any of the research participants personal or company information or any other identifying characteristics. For example, designated alphanumeric codes to ensure confidentiality will include P1, P2, and Hospital-1. I will keep all information in a locked password-protected fire-rated safe for a period of 5 years, accessible only to me. After 5 years of the research completion, I will destroy all research information.

Research Dissemination

I will publish the study report in a peer-reviewed journal for a variety of readers. The participants who participate will receive a summary of the research findings.
Potential benefits of this project are a better understanding of security strategies to reduce cyberesecurity breaches in hospital's IT environment.

We understand that our organization's responsibilities include: provide email addresses and contact phone numbers for potential research participants, accommodate the potential participants to consent to the study, to interview with the researcher, and to review a summarized copy of the interview data to validate accuracy for data analysis use. We reserve the right to withdraw from the study at any time if our circumstances change.

I confirm that I can authorize the approval for the research in this setting.

I understand that the data collected will remain entirely confidential and may not be provided to anyone outside of the research team without permission from the Walden University Institutional Review Board.

Sincerely,

_____

Name:
Contact Information

This form can be signed via email if the accompanying email is attached with the signer's personal email address included. The form cannot be completed by phone, rather should be handled via post.

Walden University policy on electronic signatures: An electronic signature is just as valid as a written signature as long as both parties have agreed to conduct the transaction electronically. Electronic signatures are regulated by the Uniform Electronic Transactions Act. Electronic signatures are only valid when the signer is either (a) the sender of the email, or (b) copied on the email containing the signed document. Legally an "electronic signature" can be the person's typed name, their email address, or any other identifying marker. Walden University staff verifies any electronic signatures that do not originate from a password-protected source (i.e., an email address officially on file with Walden).

Appendix B: Research Participants Email Introduction

Hello [potential participant's name],

My name is Donovan Pottinger, a doctoral student at Walden University working to obtain a Doctor of Information Technology(DIT) degree with a specialization in Cybersecurity. I am conducting a doctoral study to explore the strategies to reduce cybersecurity breaches in hospitals.

You are receiving an invitation to be part of this research because you are an IT leader who has adopted cybersecurity strategies to combat cyberattacks on the hospital patients and customers' sensitive information such as Protected Health Information (PHI). I understand time can be a constraint, but the face-to-face and telephone interviews will be an hour each. The first interview will be a face-to-face meeting in person or through Skype to extract research data while the second interview will be a telephone interview to review the accuracy of the summarized transcribed interview data or include any other additional new information. I believe your participation can contribute vital knowledge towards this project and existing literature. If you agree to participate, you will receive a summary of the study findings. Potential benefits of this project are a better understanding of security strategies to reduce cyberesecurity breaches in hospital's IT environment. The interview will take place at a time, date, and location outside your company's workplace and time that you and I agree to conduct the interview.

If you are interested in participating in the study, please take few minutes to complete the attached consent form and return by email. Additional information about the study is available in the informed consent form. After receipt of your email, I will call you to set up an interview time suitable to you. Please contact me at (404)593-3440 if you have any questions. Appreciate your participation in advance as I look forward to speaking with you.

Thank you

Donovan M. A. Pottinger
Walden University Doctoral Student

Appendix C: Interview Protocol

1. Schedule face-to-face (Skype or in-person) interviews for the first interviews and telephone interviews for the follow-up interviews with participants at suitable times, dates, and locations outside the participants' company workplace and time.
2. Prepare notes as reminders about the business problem under study to ensure extraction of quality research data at the interviews to address the research question.
3. Each interview will begin with an icebreaker conversation to engage the participant and create a relaxed environment.
4. Provide each participant with a brief overview of the purpose of the study and share my intent for the interview and confidentiality guidelines before I start asking interview questions.
5. Ask the 10 semistructured interview open-ended questions for the study to each participant in the same order.
6. Take note and clarify participants' nonverbal communication such as gestures, the tone of voice, and facial expressions.
7. Ask probing questions when necessary to ensure the participants provide thorough responses to the interview questions.
8. Monitor the interview time to ensure adequate research data are extracted from the participants using the interview questions.
9. Document reflective notes throughout the interview process.
10. Conclude by thanking the participants for their time and inform the participants of the follow-up interviews to conduct member checking.

Appendix D: Interview Questions

With respect to the actual interview questions meant to capture the "what, how, and why" aspects of cybersecurity within the hospital, I can map or group such questions into three sets of categories of interview questions:

What Cybersecurity Software, Hardware, and Network Environment are utilized?

1. Describe what software cybersecurity solution you have to protect your hospital's IT infrastructure against phishing, malware, and hacking.
2. Describe what hardware cybersecurity solutions are implemented to tackle hardware vulnerabilities such as weakness in computer chips.
3. Describe what common networking security measures you have implemented in your network environment to combat cybersecurity threats.

How is Cybersecurity Implemented?

1. How do you implement cybersecurity's best practices using dedicated personnel for prevention, detection, and combating comprised situations?
2. How can technology executives implement the best practices of data security with policies and procedures within the hospital IT environment?
3. How easily can intelligence about malware be distributed and acted upon within your hospital's IT infrastructure?
4. How do you implement a cybersecurity framework to investigate and remediate any cybersecurity breach in your hospital's IT environment?

Why is Cybersecurity Important to Your Hospital?

1. Are the increased risks associated with improvements (such as EHR) of IT technologies always significant to consider in your hospital? Why or Why not?
2. Do you use cost-benefit analysis techniques to compare the cost and benefits of cybersecurity implementation in your hospital IT infrastructure? Why or Why not?
3. Do you perform risk management of your hospital such as choosing cybersecurity insurance, for example? Why or Why not?

Appendix E: TranscriptionPuppy Privacy Agreement

About Quality Control and Privacy

How do you protect my information privacy?

“We're happy to sign a non-disclosure agreement before beginning work on your transcription.

Your credit card information is encrypted and securely transmitted to the credit card processor / bank and is not stored on our servers.”

Appendix F: List of 31 Codes in ATLAS.ti From Deductive and Inductive Coding

Name	Groundedness	Density	Groups
Build a robust cybersecurity policies and procedures	58	1	Theme 1
Check vulnerability and risk advisory feeds	25	1	
Conduct Regular Cybersecurity Risk Assessments	75	1	Theme 3
Continue Security Education Training and Awareness (SETA)	85	1	Theme 5
Create An Incident Response Plan	53	1	Theme 7
Cultivate Security Awareness Culture	19	4	Theme 5
Cultivate Security Education Training Awareness	6	1	
Do System update/Patching	15	1	Theme 2
Encrypt all Data at Rest and In Transit	21	3	Theme 6
Ensure Adherence to HIPAA Rules at Every Stage	4	0	
Ensure Adherence to Top Cybersecurity Framework	86	2	Theme 1
Ensure Data Backup	12	0	Theme 4
Ensure strong password	28	1	Theme 2
Establish A Cyber Risk Management Committee	0	0	
Follow security influencers and professionals	1	1	Theme 7

Hospital Cybersecurity Strategies	0	7	
Identify cybersecurity risks	101	0	
Implement adequate and effective cyber controls	30	6	Theme 2
Implement Encryption Standard	35	1	
Implement user two-factor/multifactor authentication	5	1	Theme 2
Keep Abreast with Cybersecurity News and Risks	28	6	Theme 7
Keep current with cyber threat intelligence	39	1	
Maintain an Air Gap Technique Backup	28	1	Theme 4
Plan for Incident Management	36	1	Theme 3
Promote a Collaboration Between government and manufacturers	1	0	
Protect access to healthcare data	58	1	Theme 2, Theme 6
Protect access with efficient identity management	28	1	Theme 2
Protect your sensitive data	5	0	Theme 4, Theme 6
Raise cybersecurity awareness	31	1	Theme 5
Understand the Hospital IT Infrastructure	6	0	
Use secure Internet protocol	19	1	

Appendix G: List of Documents From Hospital-3 (Case3): Policies

Study Name	Word Document: Name of Policies
H3D5	CW IS SEC 101 Information Security Management Policy
H3D6	CW IS SEC 102 Endpoint Protection Policy
H3D7	CW IS SEC 103 Portable Media Security Policy
H3D8	CW IS SEC 104 Mobile Device Security Policy
H3D9	CW IS SEC 105 Wireless Security Policy.docx
H3D10	CW IS SEC 106 Configuration Management Policy
H3D11	CW IS SEC 107 Infrastructure Vulnerability Management Policy
H3D12	CW IS SEC 108 Network Security Policy
H3D13	CW IS SEC 109 Transmission Security Policy
H3D14	CW IS SEC 110 Password Management Policy
H3D15	CW IS SEC 111 Access Control Policy
H3D16	CW IS SEC 112 Audit, Logging, and Monitoring Policy
H3D17	CW IS SEC 113 Information Security Education, Training, and Awareness Policy
H3D18	CW IS SEC 114 3rd Party Assurance Policy
H3D19	CW IS SEC 115 Information Security Incident Management Program Policy

H3D20	CW IS SEC 116 Business Continuity and Disaster Recovery Policy
H3D21	CW IS SEC 117 IT Risk Management Policy
H3D22	CW IS SEC 118 Physical and Environmental Security Policy
H3D23	CW IS SEC 119 Data Protection and Privacy Policy
H3D24	CW IS SEC 120 Acceptable Use Policy