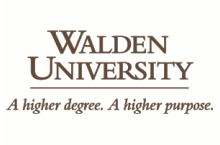

2020

Cybersecurity Using Risk Management Strategies of U.S. Government Health Organizations

Ian Cornelius Wilkinson
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Ian Cornelius Wilkinson

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. Cheryl Waters, Committee Chairperson, Information Technology Faculty
Dr. Gary Griffith, Committee Member, Information Technology Faculty
Dr. Bob Duhainy, University Reviewer, Information Technology Faculty

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

Walden University
2020

Abstract

Cybersecurity Using Risk Management Strategies of U.S. Government Health Organizations

by

Ian Cornelius Wilkinson

MA, Webster University, 2015

BS, University of Maryland University College, 2012

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

Student ID: A00705871

December 2020

Abstract

Seismic data loss attributed to cybersecurity attacks has been an epidemic-level threat currently plaguing the U.S. healthcare system. Addressing cyber attacks is important to information technology (IT) security managers to minimize organizational risks and effectively safeguard data from associated security breaches. Grounded in the protection motivation theory, the purpose of this qualitative multiple case study was to explore risk-based strategies used by IT security managers to safeguard data effectively. Data were derived from interviews of eight IT security managers of four U.S. government health institutions and a review of relevant organizational documentation. The research data were coded and organized to support thematic development and analysis. The findings yielded four primary themes: effective cyber-risk management strategies: structured, systematic, and timely cyber risk management; continuous and consistent assessment of the risk environment; system and controls development, implementation, and monitoring; and strategy coordination through centralized interagency and interdepartmental risk management. The key recommendation based on the study findings is for IT security managers to employ cybersecurity strategies that integrate robust cybersecurity controls and systematic processes based on comprehensive risk management. The implications for positive social change include the potential to positively stimulate patient trust and confidence in healthcare systems and strengthen healthcare professionals' commitments to ensure patient privacy.

Cybersecurity Using Risk Management Strategies of U.S. Government Health Organizations.

by

Ian Cornelius Wilkinson

MA, Webster University, 2015

BS, University of Maryland University College, 2012

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

Student ID: A00705871

December 2020

Dedication

I dedicate this study to my daughters Karina, Ceilia, and Haruka as a representation of what can be accomplished through faith, hard work, and dedication.

Acknowledgments

First and foremost, I would like to give thanks, honor, and glory to God for giving me the strength and endurance through times of adversity, trials, and tribulations to pursue my passion beyond reaching my goals to achieving my dreams. I would also like to thank my family, friends, and loved ones for their patience, support, and encouragement throughout my journey. Finally, I would like to thank my chair, committee, URR, and the faculty and staff at Walden University for their instrumental mentorship and guidance toward this accomplishment.

Table of Contents

List of Tables

Section 1: Foundation of the Study

Background of the Problem

Data breaches, malicious activities resulting in a multibillion-dollar range of annual losses, involve incidents that derive from unauthorized access and subsequent compromise to the confidentiality, availability, and integrity of sensitive data. A rapid growth in cybersecurity incidents including data security breaches affecting the healthcare industry have become an increasing concern for information security professionals worldwide. Although the healthcare sector is vulnerable to cyber attacks targeted at infrastructure, services, and interconnected devices, the impact of healthcare data breaches may be more profound than threat vectors experienced with other prominent industries when accounting for risks to patient safety and wellbeing (Ahmed et al., 2019).

The protection motivation theory (PMT) was founded on the premise of understanding fear appeal and its contribution to comparable risk management. This concept can be used in information technology (IT) enterprise architecture and system development lifecycle (SDLC) constructs to reduce security breaches. The theory combines risk-driven security and risk management functions motivated by three mediational processes that account for the amount of risk, probability of risk realization, and efficacy of protective response. Adopting a concept of operations based on the PMT in the organization provides information security managers in the healthcare sector the capability to integrate enterprise-level cybersecurity and enhance the risk management experience through defined roles and responsibilities. In that regard, the integration of the

PMT concept facilitates improvement in IT security and strengthens the processes of risk management in an organization.

Problem Statement

Seismic data loss attributed to cybersecurity attacks has been an epidemic-level threat currently plaguing the U.S. healthcare system and costing hospitals upwards of $7 million per incident (Jalali & Kaiser, 2018). Between 2009 and 2016, the Office of Civil Rights reported 27 Veterans Affairs (VA) hospitals had incurred breaches of protected health information (PHI) that affected 500 or more patients (Cortelyou-Ward et al., 2018). The general IT problem is IT security managers are not adequately addressing challenges to securing patient data accessed from healthcare IT infrastructures. The specific IT problem is that some IT security managers lack cybersecurity risk strategies to effectively safeguard PHI and personally identifiable information (PII) from data breaches concerning U.S. government health organizations.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the cybersecurity risk management strategies effectively used by IT security managers to safeguard PHI and PII from data breaches concerning U.S. government health organizations. The targeted population consisted of the IT security managers of four medium-sized government health institutions located in the Midwest United States. The findings of this study may contribute to social change by positively stimulating patient trust and confidence in healthcare systems and strengthening the commitments of healthcare professionals to ensure patient privacy.

Nature of the Study

For this study, I chose to use a qualitative research methodology as the most appropriate approach. Qualitative methodologies are dependent on the interpretation of multisourced qualitative data within a natural setting, which is thematically synthesized by the use of inductive reasoning and shaped by onto-epistemological assumptions of the researcher (Bansal et al., 2018). Qualitative methods are inferred when a researcher seeks to understand and correlate associated themes in the study (Bamberg et al., 2018). This method was best suited for this study because the research involved exploring strategies of IT security managers using thematic synthesis within a natural environment to gain a better understanding of patterns and commonalities associated with VA healthcare IT security postures. Presumably, more profound insight into these thematically linked criteria surrounding IT security postures may promote consequential IT security strategy development. The quantitative methodology and associated designs (descriptive, correlational, experimental, and quasi-experimental) are more focused on numerical values and variable relationships produced in a controlled environment (Bouikidis & Rutberg, 2018). This study did not focus on numerical values or variable relationships in a controlled environment. Therefore, the quantitative methodology and its designs were not appropriate for this study.

Moreover, in this this study I explored a natural environment, which is usually representative of a qualitative methodology versus a controlled environment exploration typical to the quantitative methodology and mixed methods methodology. Mixed methods are used to research the employment of both natural and social sciences as a

mixture of quantitative and qualitative methodologies (Maxwell, 2015). Therefore, the mixed methods methodology was not appropriate for this study, as this study did not employ both quantitative and qualitative methodologies.

This research followed a multiple case study design, and I used a varied number of sources to collect and synthesize the data into a well-rounded case analysis. Alpi and Evans (2019) stated that the primary emphasis of the case study is to understand the *how*, the *why*, and the *what* surrounding the exploration in time and space of a particular phenomenon. In this study I sought to understand and synthesize cybersecurity risk management strategies used in cases particular to government healthcare. Also, with this study I strived to understand the use of various strategies and how the strategies promote optimal IT security practices.

The narrative research design collects research data and formulates them into a story or stories for analysis (Polkinghorne, 2006). Therefore, the narrative research design was not appropriate because this study was not focused on individual stories for IT security strategy analysis. Ethnographic designs focus on research that reports on experiences of a particular group differentiated by like characteristics such as origin or ethnicity (Walford, 2018). Therefore, the ethnographic research design was not appropriate because this study did not use interpersonal stories related to cultural settings to research IT security strategy. Phenomenology designs are used to explore a phenomenon such as perceptions and meanings through general analysis (Boz & Daglı, 2017). Therefore, a phenomenology research design was not appropriate because this

study did not explore the strategies used by IT security managers within VA health organizations through the essence of generally analyzed shared experiences.

Qualitative Research Question

RQ: What are some security strategies used by IT security managers to effectively safeguard PHI and PII from data breaches concerning U.S. government health organizations?

Interview Questions

1. What experiences have you had implementing risk management strategies toward the IT security and administration of government health organizations?
2. What were some of the technologies you've used and your perceptions of those technologies to secure PII and PHI?
3. How do you identify threats to protected health data, and how are those threats mitigated?
4. What procedures and mechanisms have you used to decrease vulnerabilities and ensure health information security software and technologies have the latest software patches or firmware?
5. What procedures are in place to notify users or shareholders of potential or realized breaches of data?
6. What policies and procedures are in place to ensure compliance with state, government, and organizational laws, policies, guidelines, and regulations regarding PHI?

7. How are the information systems of the organization and the associated data processed within the organization categorized to support adequate selection and implementation of security controls?
8. How are the security controls assessed and monitored after implementation, and what are the processes in place to support periodic assessments to sustain the security posture of the organization?
9. What are the procedures for authorizing an information system, and what position or organizational level is responsible for authorizing information security systems on the network?
10. Is there anything else that you would like to include concerning security strategies for cybersecurity that was not covered?

Conceptual Framework

The conceptual framework used to inform this study was the PMT. The intent of the Rogers's (1975) study was to investigate the outcomes of fear appeals on attitude change and to examine influencing factors associated with appropriate courses of action to prevent the noxious occurrence. Rogers established the theory as a singular part of more comprehensive expectancy-value theories and proposed that the three critical components of the PMT appeal to the natural fear of unfavorable outcomes. The three components are described as (a) the magnitude of adversity of a depicted event, (b) the event's probability of occurrence, and (c) the effectiveness of a protective response (Rogers, 1975). The participating communication variables of the PMT correspond to cognitive thought processes that influence attitude change. Simply stated, fear of realized

risk drives protective and proactive risk responses; the higher the fear of unfavorable consequences, the more persuasive the need for a countering protective response. Rogers also highlighted that fear is a relational construct that is stimulated in response to an event, and it is an emotion of motivation often leading away or escape from a noxious event. According to Rogers, the PMT is driven by the perception of relevant risk and the related increase in the use of protective measures under duress or concern that is often contributed to previous experience or incident. The foundations of the PMT have been used to influence and emphasize safety campaigns to promote proactive and reactive change by invoking the cognitive mediating processes to evaluate the noxiousness, probability, severity, and effectiveness of a risk response. Subsequently, the most prudent risk response plan is adopted and placed into action driven by protection motivation.

The conceptual framework of Rogers's (1975) PMT was relevant to this study by aiding exploration of the fundamental concepts of risk management as they related to the actions of safeguarding PHI and PII influenced by the inherent fear of adverse consequences such as data breaches or ransomed data. This study used the groundwork of the PMT in terms of understanding fear appeals or the relevant consequences of realized negative risk to support the appropriate amount of protection motivation arousal and subsequent directed activity or response. Imposed upon the information security lifecycle approach and associated motivated information protection concepts, the PMT helps IT security managers develop an understanding of the effectiveness of cybersecurity risk strategies of government health organizations. Cybersecurity and risk management platforms in this study represent government health information systems outlined in IT

health security strategies. The PMT informed this study by relating the risk management and security influenced concepts explored by Rogers (1975) to the overall protection and privacy of health-oriented data and secure health information management today.

Operational Definitions

Electronic health records (EHR): The digital form of a patient's medical care chart is created and managed by authorized personnel, and it provides pertinent clinical health data of the patient except for treatment history (Office of the National Coordinator for Health Information Technology, 2019).

Healthcare information technology (HIT): Healthcare IT refers to the application of data and information processing, retrieval, storage, and sharing, which is facilitated by information technology hardware and software in support of healthcare (Edenharter et al., 2018).

Health Insurance Portability and Accountability Act of 1996 (HIPPA): HIPPA is the compliance model for health information protection enforced by the U.S. Department of Health and Human Services, which ensures the security of specific electronic health data transactions (Vanderpool, 2019).

Protected health information (PHI): PHI is confidential patient information that pertains to the health history and condition of a patient and inherently would have a high-risk potential if a particular threat were realized considering the sensitivity of the information managed, stored, or particularly in transit (Du et al., 2018).

System development life cycle (SDLC): SDLC describes the framework and conceptual model that makes up the five primary phases of planning, analysis, design,

implementation, and maintenance of information system project development (Atkins et al., 2017).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions in a study are influencers over which the researcher has no control that assist the researcher in comparatively examining and appropriately interpreting the findings of the study (Kirkwood & Price, 2013). One of the primary assumptions for this study was that the interviewees were fully qualified and truthful in providing answers to the interview questions. A complementary assumption was that no irregular external authorities or atypical stimulus influenced the answers of the interviewees. Another significant assumption was that the target population subject to this study was an accurate depiction of the greater population represented.

Limitations

Limitations of a study are conceivable constraints outside of the control of the researcher that have the potential to impact and influence the findings of the study (Aguinis et al., 2013). One primary limitation was managing uncertainty with an educated estimation due to the inability to access and assess the total population that the study represents. Another limitation focused on virtually conducted interviews and the inability to conduct all interviews in person to observe facial expressions, body language, and other nonverbal communication.

Delimitations

Delimitations are choices within the control of the researcher to limit the scope of the study by setting predetermined boundaries (Fountouki & Theofanidis, 2018). The scope of this study was determined by the use of a qualitative multiple-case study to explore the strategies effectively used by IT security managers to safeguard PHI and PII from data breaches concerning U.S. government health organizations. The associated delimiting factor was that only IT security managers in the Midwest United States with relevant experience safeguarding PHI and PII within a government health organization participated.

The Significance of the Study

Contribution to Information Technology Practice

This study is significant to IT practice to the extent that it may provide information security managers some successful strategies to fill gaps in practice and application in the government healthcare environment to mitigate security risks concerning PHI and PII. Understanding these strategies that are well defined and practiced by IT security managers may provide an effective conduit for integrated secure health information management technologies and positively influence organizational culture. Also, this study may be significant for IT security managers to identify secure information technology practices in the health data and information management field.

Implications for Social Change

This study is significant to society on a large scale by potentially improving and standardizing methods for electronic health data management in support of healthcare

professionals. Consequently, the employment of the data protection and risk management methods detailed in this study could provide the medical community and patients with greater support and services through the promotion of protected access to individual health information. Therefore, this study may promote social change by positively stimulating patient trust and confidence in healthcare systems and strengthening the commitments of healthcare professionals to ensure patient privacy.

Review of the Professional and Academic Literature

A significant increase in complexity of hardware and software that includes firmware and other types of interconnected systems, devices, and platforms that assist in providing medical support and services throughout government health organizations, the attack vectors, attack surface, and opportunities for a cyberattack have greatly advantaged malicious actors and cyber-adversaries (Ahmed et al., 2019). In this literature review, I explored the challenges faced by IT security professionals maintaining the confidentiality, availability, integrity, and the overall protection of data from hackers and other actors who threaten and prey on vulnerable IT systems. I also explored the elements of cyber risk as they pertain to the government-sponsored healthcare industry. Reviewing risk management practices in terms of processes implemented, I investigated methods used by IT security professionals to control the probability of realized exfiltration and exploitation of healthcare data. This review used relevant articles from peer-reviewed journals, government periodicals and publications, and books as resources for conceptual development.

The literature review opens with an overview of healthcare information technology and the associated challenges to managing healthcare IT security risks. In the review I synthesize supporting literature that outlines the components of IT risk management relative to the PMT, IT security infrastructure, and information security development. Throughout this section, I include and examine the critical factors of successful IT risk management strategies and their associated challenges. I also focus on the literature supported by the conceptual framework of the PMT as the foundation of this study. Complementary and contrasting theories are included, along with the application and adoption of supporting frameworks that were built on the PMT construct and used in the healthcare industry. Lastly, I highlight how the information in the reviewed literature supported the present study.

My review of the literature that informed this study was completed using the Walden University library, Google, EBSCOhost, Google Scholar, OMICS International, ProQuest, Ike Skelton Combined Arms Research Library (CARL) Digital Library, and various academic studies and dissertations. All peer-reviewed scholarly journals were verified of their refereed standing using detailed information provided in the Ulrich database. Comprehensive research enabled me to study the literature relevant to my conceptual framework, which highlights elements of risk management as it pertains to authorizing and assessing IT systems security and IT security management. Of the total of 215 sources used throughout this study and relevant to my research, 199 (92.6%) were peer-reviewed or from U.S. government sources and 196 (91%) were published within 5 years or less of the anticipated chief academic officer approval date. My literature review

is comprised of 120 sources. Of the sources I collected for the literature review, 106 (88%) were peer-reviewed, 103 (86%) were published works within 5 years or less of the anticipated chief academic officer approval date, and 72 (60%) were seminal works. As part of the scholarly groundwork, the information gathered for this study assisted me in exploring and analyzing the cybersecurity risk management strategies used by IT security managers to safeguard PHI and PII from data breaches concerning U.S. government health organizations.

My primary strategy for searching the literature was to search based on the literary themes of IT risk management development and IT security. I then subdivided both the IT risk management and the security searches into manageable parts. I conducted my search for themes of the IT risk management section based on the topics of preparation activities and the categorization of systems. I also conducted my search for themes of the security section based on the topics of selection, implementation, assessment, authorization, and monitoring of systems and security controls.

Analysis and Synthesis of Conceptual Framework Literature

In this section of the literature review, I provide my synthesis of the supporting literature that outlined the context and components of the PMT as my conceptual framework. I also include critical analysis with supporting and contrasting theories and conceptual models that are comparative to the PMT. Included in my analysis, I also compare and contrast various points of view and the relationship of the study to previous research and findings. Lastly, I reflect on the challenges that some health organizations face regarding IT security. Supporting my conceptual framework as a foundation of the

IT security infrastructure and information security development in U.S. government health organizations, the thematic consensus concerning mitigating threat factors was derived from conducting a comprehensive review of studies on IT risk management.

There is a continual need for health organizations to have an overarching risk management strategy to strengthen their approaches to cybersecurity breach prevention, address cybersecurity concerns, and minimize risks. Ammenwerth and Leber (2017) highlighted cautionary lessons learned from processing patient personal health data with technological resources in health organizations. The purpose of their research was to develop a collection of measurements and indicators necessary to effectively support the IT-based risk management process in health facilities using a qualitative and quantitative Delphi study. The underlying assumption associated with their research was the possibility of identifying practice measures that a hospital should implement that are relevant to IT risk management and the reliability of the data collected that is used to measure impacts.

Application to the Applied Information Technology Problem

Large amounts of data loss have been attributed to recent cybersecurity attacks targeted at vulnerabilities in systems and processes of the U.S. healthcare system, costing hospitals as much as $7 million per incident (Jalali & Kaiser, 2018). The Office of Civil Rights reported 27 VA hospitals had incurred breaches of PHI, which affected 500 or more patients between 2009 and 2016 (Cortelyou-Ward et al., 2018). Since the advent of cyber-based attacks in the 1970s, cyberthreats have exponentially increased with technological advances. Cyber threat actors have found particular focus over recent years

toward exfiltrating or ransoming health organization and patient health data (Frederick et al., 2017). The literature expressed themes that outlined the need for a risk-based strategy as IT security managers address cybersecurity in U.S. government health organizations. The purpose of this qualitative multiple case study was to explore the cybersecurity risk management strategies effectively used by IT security managers to safeguard PHI and PII from data breaches concerning U.S. government health organizations.

Several authors in the reviewed literature concurred that the PMT uses a broad risk-based conceptualization that addresses cybersecurity concerns and challenges through three cognitive appraisal processes. The cognitive appraisal processes of the PMT and potential themes are: (a) assist executive-level staff and IT security managers to prepare the organization for system-level integration; (b) categorize information according to loss impacts; and (c) select, implement, and assess appropriate controls. The PMT also assists senior managers to authorize the system and controls and assists IT managers to monitor the system and associated controls for effectiveness. Boyle et al. (2018) proposed that there is a foundational relationship between threats and countermeasure awareness (CA) with the fear arousal elements of the PMT, detailed as perceived vulnerability, perceived severity, self-efficacy, response costs, and response effectiveness. The Boyle et al. (2018) research demonstrated that all PMT elements, excluding perceived vulnerability, considerably affect security behavior.

There are several themes of conducting thorough and periodic risk assessments to maintain a complete and accurate picture of the organizational security posture throughout the data and information lifecycle. Literature themes suggested that the PMT,

complementary theories, frameworks, and regulatory guidelines and standards are relevant for present-day application as they assist IT security managers of U.S. government health organizations in data breach prevention (Ahmad et al., 2019; Ahmed et al., 2019; Alaydrus et al., 2017; Baldini et al., 2019; Keenan et al., 2016; Rogers, 1975). This relevance was accomplished through the development of a risk-based context and setting the priorities for cybersecurity risk management and promoting ongoing privacy and security (Aljohani et al., 2018; Kim et al., 2018; Johnson & Kwon, 2015; Rezaeibagha et al., 2015; Small & Wainwright, 2018). IT security managers may choose to adopt complementary frameworks to support the security-based concepts of the PMT and decrease the exploitation of data resources held within the protection boundaries of government health organizations (Abie & Boudko, 2019; Abramson et al., 2019; Belaissaoui & Elkhannoubi, 2015; Cagliano et al., 2015; Cram et al., 2017; Gan et al., 2020; National Institue of Standards and Technology Joint Task Force [NISTJTF], 2018). Most project management frameworks from organizations such as the Project Management Institute (PMI) and Axelos explored and detailed elements of risk management processes pertinent to identifying and responding to risks (Cram et al., 2017; Gan et al., 2020; Grohmann, 2018; Keenan et al., 2016; Monken et al., 2017; Thompson & Zandona, 2017). Identifying and responding to risks are also key elements of understanding and controlling cyber-oriented threats that are relevant to the security posture of an organization (Ahriz et al., 2017; Biskupek, 2018; Cagliano et al., 2015; Keenan et al., 2016; Moeini & Rivard, 2019). Interpreting themes found in project management frameworks, Ahriz et al. (2017) believed IT security and IT risk managers

should address risk management strategy and risk response planning early in the project lifecycle. Achieved through known IT and IT security risk management standards and models, the focus on IT risk will enhance the IT project investment and provide optimal alignment with organizational strategy (Ahriz et al., 2017). Typically performed at the start of projects in the planning phase, Boonjing and Pimchangthong (2017) stated that risk identification and risk response planning has a greater influence on IT project success than forecasting equations alone and is instrumental in performing comprehensive risk management. Expanding on this concept, Biskupek (2018) asserted that innovative IT and IT security projects are subject to greater levels of risk; a planned and methodical approach to risk response and actively managing risk with commonly known methodologies and tools are pillars of project success. Relevant to this study were the PMT considerations IT security managers of U.S. government health organizations should have regarding the planning and systematic implementation of IT security projects, specifically regarding risk identification and risk response planning.

The basis of the PMT is the observed correlation between perceived magnitude and potential of noxious events and protection motivation to properly respond to those events. Hanus and Wu (2016) examined the security behaviors relating to security risks and influenced by the objectives of the PMT through an understanding of threat awareness (TA) and CA. The authors focused their research on positive outcomes of TA and CA using the PMT as a catalyst. They concluded that concentration on both TA and CA result in increased security consciousness and the subsequent implementation of protective behaviors that are influenced by successful security training related to the PMT

concept of avoiding or minimizing the risks of negative events. Boyle et al. (2018) also studied the behavioral effects of security awareness and elaborated further stating that there is a direct correlation between threat and countermeasure awareness and the elements of the PMT. The elements included (a) perceived severity of a noxious event, (b) perceived vulnerability, (c) efficacy of self, (d) efficacy of response, and (e) the associated cost of that response. Boyle et al. (2018) expressed that IT security managers and security professionals alike are the custodians of the IT security posture of the organization. As such, their security constructs are the primary target for hackers pursuing unauthorized access to sensitive data of the network within the organization (Boyle et al., 2018). The authors concluded that the PMT is an effective perspective to adequately predict the cybersecurity risk responses of IT security managers in terms of security behaviors and developing and maintaining a custodial relationship to critical elements of the computing environment through security awareness and risk management. Baronienė and Žirgutis (2017) concentrated their research on data security problem-solving decisions through a technical lens, the PMT, and security standards adoption. The authors mentioned the need for IT security managers to act based on the fear of compromise influenced the forecasting of the trends of data security concerns, which include unintentional consequences of state intervention, big data risks, mobility risks, increased cybercrime, and a gap in IT security skills. Baronienė and Žirgutis (2017) stated that a supportive methodology of ensuring data security is to develop data of certified information management systems through a formalized certification process of the organization. Cram et al. (2017) analyzed considerable research concerning the study

of supporting conceptual frameworks for organizational information security policies. Their research suggested that past research about the influence of the organization and individual employees on policy compliance stemmed from commonalities between the foundational theories of the PMT, general deterrence theory (GDT), and the theory of planned behavior.

General Deterrence Theory

Jervis (1979) revisited the 18th-century deterrence theory proposing the active relationship between behavioral results on implementing swift and severe consequences and successful deterrence to influence compliance or prevent certain activity engagements. Herath and Rao (2009) concluded that there is a correlation between the PMT and the GDT through observed negative connotations associated with the severity of the consequences. The concepts of the deterrence theory proved to be more effective as deterrence of negative behavior, but less effective with encouraging positive behavior such as compliance. Guo and Yuan (2012) found greater success in using a more positive approach through compliance while leveraging multilevel interagency developed sanctions to influence the effects of deterrence regarding information security standards and policies. The authors recognized that the more positive aspect of this internal department sanction development approach was seen more favorably amongst the staff under the assumption that the majority maintains an active vote toward sanction development. The concepts of the GDP are relevant to this study regarding the implementation of effective means of deterring data security breaches.

Theory of Planned Behavior

The perceptions and points of view of the PMT differ within varying fields of study and also differ considering the evolution of risks and evolution of the emphasis placed on effectively and efficiently managing risk as it relates to cyber and information security in general. Gan et al. (2020) states the investors of risk-based constructs that use the PMT foundational concepts perceive the methodologies and approach positively and in direct alignment with risk-based cybersecurity practices that have practical implications for both organizations and regulatory bodies. However, there are opposing theories to the PMT that investigate risk differently than observing appropriate action influenced by protection motivation as a result of avoidance of a perceived noxious event or series of events. One such theory is the theory of planned behavior (TPB). As another foundational theory to risk management practices that contrasts with the PMT, the TPB is part of a series of theories that find roots in the conceptualizations of expectancy-value. Unlike the PMT which seeks to understand human behavior based on the prevention, avoidance or relevant and comparable counteraction of noxious events, the TPB focuses on the development of goal-oriented instinctive behavior. Ajzen (1985) proposes that human behavior is the product of formulated plans and is more or less a result of semi-instinctual routines as tasks to achieve an objective or highly developed skills that no longer require forethought to perform. TPB is relevant to this study given the aspects of risk management integration by (a) inspiring a systematic approach to cybersecurity by cultivating routine practices to assess vulnerabilities in IT systems and associated networks; (b) proposing and implementing viable control methods; and (c) accrediting,

certifying, and continuously monitoring IT systems and associated vulnerabilities as a means of supporting a risk-controlled computing environment.

Several cyber security-based and risk-based frameworks, methodologies, standards, and related theories, directly and indirectly complement the concepts of protection motivation that govern risk management as a derivative of the PMT. Moreover, cybersecurity risk management undertakings are designed to support the protection of IT assets from cyber threats. The PMT conceptualization motivates IT security managers in government health organizations to adopt supporting cyber risk standards and frameworks to aid in the development and facilitation of a shared understanding and enhance the organizational information security posture (Rogers, 1975). Two of the most prominent risk management frameworks are the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) and the Information Systems Audit and Control Association (ISACA) Control Objectives for Information and Related Technology (COBIT).

Risk Management Framework

NIST (2018) outlines the correlation between the processes of risk management and cybersecurity and each respective framework is gained through the understanding of relevant risk, risk tolerance, and associated risk responses to effectively prioritize cybersecurity controls and activities and make informed decisions. The authors detailed that cybersecurity is the risk-based method that strengthens the relationship between business drivers and cyber activities (NIST, 2018). Using the corresponding element of fear aroused risk response detailed in the PMT, the RMF generally consists of three

sections: the Framework Core (cybersecurity activities), the Framework Implementation Tiers (organizational view of cybersecurity risk and associated risk responses), and the Framework Profiles (organizational security posture based on business requirements) (NIST, 2018). The authors of the framework conclude that IT security managers will benefit in establishing or improving the cybersecurity program of an organization through the iterative processes of cybersecurity. The process includes defining and prioritizing assets, orienting the systems and assets to meet regulatory requirements and identifying relevant risks, creating a current security profile, conducting a risk assessment, creating a goal-oriented security profile, examining security gaps, and implementing a relevant action plan (NIST, 2018). Several other cyber security-based frameworks focused on a risk-based approach to effectively understand and respond to cyber threats and communicate the cybersecurity risk management plan with pertinent stakeholders.

Cybersecurity Framework

Abie and Boudko (2019) suggest that health organizations should adopt a dynamic cybersecurity framework that is integrated to protect multifaceted healthcare ecosystems and positively influence efficiency, resilience, privacy, and overall information security. Considering exploitation time threat actors have, critical infrastructure dependency vulnerabilities, and cybersecurity system limitations, the authors use modeling and analysis to stimulate their evolutionary game theory and machine learning approach to explore their dynamic cybersecurity framework (Abie & Boudko, 2019). The authors conclude that the possibility of a dynamic cybersecurity strategy is dependent upon the refinement of the Nash Equilibrium to allow cybersecurity

system convergence on an Evolutionary Stable Strategy and prevent alternative mutant strategies (Abie & Boudko, 2019). Abraham, Chatterjee, and Sims (2019) highlight challenges of the healthcare industry regarding security preparedness to respond to cyber threats, the vulnerabilities of interconnected medical equipment, IT security manager complacency, and the tasks of meeting various compliance requirements. The authors suggest an organizational adoption of a comprehensive cyber resilience strategy that deliberately and proactively integrates methods to undertake cybersecurity risk management in health organizations (Abraham et al., 2019). The authors conclude with an emphasis on the importance of IT security professionals in health organizations to understand the cybersecurity risk posture of the organization by identifying business operations, inventorying associated assets, and assigning a relevant risk impact score and controls accordingly (Abraham et al., 2019). Using the Cybersecurity Framework (CSF) concept, Grohmann (2018) affirms that the application of the cost-benefit analysis given the situation of the organization dictates expectations of security controls planned for and implemented and the level of risk an organization is expected to accept. The author also addresses the NIST aspirations of provisioning for privacy engineering and specific skillsets of future cybersecurity personnel. (Grohmann, 2018). The alignment of organizational risk management and cybersecurity objectives is a fundamental concept for IT security managers of government health organizations to continually consider.

Control Objectives for Information and Related Technologies Framework

IT security managers may find significant benefits in adopting a support system of best practices to implement risk-based cybersecurity at an enterprise-level from end-to-

end to assist with IT governance and business decision-making. COBIT 5 is a vendor-neutral framework like the RMF which also aligns with PMT fundamentals particular to the concepts of fear appeal and risk responses. However, COBIT contrasts with the RMF as COBIT is created by ISACA specifically for IT management and governance primarily within enterprises of commercial organizations, but is often used for its risk management qualities. Whereas the RMF is a framework primarily supporting the security of information systems within the U.S. federal government to uphold federal policy and standards. COBIT also contrasts with the RMF by application, allowing business executives and IT security managers to partially implement applicable elements of the COBIT framework which encourages customization to business requirements. Recently, the COBIT framework was upgraded from COBIT 5 to COBIT 2019 to clarify terminology, further define processes, and include design factors that influence the governance of the enterprise. (Kulkarni, 2019; Thomas, 2018). Marquez (2017) states that some of the risk management supportive functions of the COBIT framework include considerations of IT and enterprise-driven goals related to a balance between negative and positive risk (opportunities) labeled risk optimization and governance of enterprise IT functionality and alignment with business needs. The author expresses that COBIT helps IT security managers overcome the challenges of gaining executive management support by facilitating realistic expectation management and ensuring that robust risk activities and processes have defined and proper accountability (Marquez, 2017). Both frameworks, representing both government and commercial business industries within their right, are derivatives of the conceptualizations found in the PMT and embody the

crucial considerations of fear appeal by integrating assessment processes which define the magnitude of noxious events and the probability of their occurrence. Both frameworks also propose methods to determine and evaluate relevant risk response methods in keeping with the components of the PMT.

Standards are primarily known as a collection of best practices developed by professionals and experts in the field of study. Standards assist an organization to effectively plan and execute operations best suited for an industry or organization. Some standards are internationally, nationally, or regionally recognized. Standards also are commonly known to be recognized only within a particular industry. Murashbekov (2019) highlighted that three of the most prominent issues with adopting some information security standards or frameworks tend to be a lack of a formalized methods to understand essential objects of the information and communication infrastructure, a lack of an information system audit plan, and a lack of information and analytical procedures to formalize information system indicators. IT security for the reasons Murashbekov (2019) outlined or similar reasons tends to implement well known IT security standards. A relevant standard complimentary to the PMT is the ISO/IEC 27001 ISM standard for industries worldwide and practiced in both a government and commercial setting. Also complimentary to the principals of the PMT are the standards that are more specific to the healthcare industry, namely the standards of Health Level Seven International (HL7), Health Insurance Portability and Accountability Act (HIPAA), and Health Information Technology for Economic and Clinical Health (HITECH).

International Organization for Standardization/ International Electrotechnical Commission 27001

ISO/IEC 27001, also known as Information Security Management, is another PMT complimentary standard created by the International Standardization Organization (ISO)/ International Electrotechnical Commission (IEC). The standard uses risk management processes to provide organizational requirements for information security management systems (ISMS) and secure information assets. Retnowardhani and Yoseviano (2018) explain that the ISO/IEC 27001 standard consists of 11 categories of security controls, 133 security controls, and 39 objectives for the security controls and uses a Plan-Do-Check-Act (PDCA) model to plan, execute, and monitor information systems. Outlining the risk management focus of the standard, the authors highlight that ISO/IEC 27001 uses 5 stages of risk management: identifying assets, risk identification, prioritizing risk, risk management develop and implement security controls, and monitoring risks (Retnowardhani & Yoseviano, 2018). The authors concluded that IT security managers will find value in implementing an ISMS using ISO/IEC 27001 to effectively determine the scope, perform gap analysis, conduct risk assessments, create policies and procedures, and setting security controls (Retnowardhani & Yoseviano, 2018).

The HL7 of 1987, HIPAA of 1996, and HITECH of 2009 are healthcare-specific standards and frameworks that are complementary to the PMT and created to mitigate risks of IT systems that protect EHRs and reduce inadequacies, and secure patient data both administratively and technically. The literature themes expressed that the main focus

concerning the HL7 standards is that of maintaining medical data integrity while in transit. However, the literature also expressed themes that detailed the focus of HIPAA as the administrative, technical, and physical controls in place to protect patient privacy using risk-based processes. Similarly, the literature expressed themes highlighting the risk-based privacy processes of HITECH but maintains an emphasis on the breach reporting requirements of healthcare IT security professionals.

Health Level Seven International

HL7 standards were designed to facilitate interoperability of information exchange between healthcare providers at the application level without sacrificing PHI security (Tian et al., 2016). There have been some strides in providing security to medical information in transit under the HL7 standard. Hu and Wang (2018) explore the concept of HL7 message validation through the use of middleware-based validating modules that use message validation rules and exact string match algorithms to improve efficiency and security specifically in terms of message integrity. Furthering HL7 security concepts, Alaydrus et al. (2017) proved the possibility of medical data exfiltration in less than three minutes using a Man-In-The-Middle (MITM) attack where attackers inject themselves in data exchanges to modify unprotected (not encrypted) or Message Digest 5 (MD5) hashed data. Alaydrus et al. (2017) advocated for the use of a hash no less advanced than Secure Hash (SHA) 512-bit to ensure attackers are unable to modify medical data in transit and maintain data integrity. IT security managers of U.S. government health organizations are usually subject to the requirements of implementing security controls to

safeguard HL7-based messages and maintaining HIPAA standards for data security under the considerations of organizational risk.

Health Insurance Portability and Accountability Act

Although the standards of HIPAA may not apply to all healthcare institutions, yet since the advent of the EHR adoption mandate for healthcare providers, there is a great majority of healthcare providers that are subject to HIPAA compliance to protect both patient privacy and patient data security. This compliance has the five key actions of periodic risk analysis, employee compliance training, implementing business associate agreements, PHI, and electronic PHI (ePHI) protection, and breach reporting (Vanderpool, 2019). HIPAA security requirements are based on the Security Rule conceptual framework which outlines the application requirements and governance of administrative (training, risk management, and roles and responsibilities), physical (physical access control), and technical safeguards (security controls and logical access control) (Mattioli, 2018). Mattioli (2018) states that the risk analysis requirements embedded within the HIPAA security management framework are in place to influence the practice of organizational periodic assessments to identify associated risks. Marting (2018) builds on this concept by stating that some of the key points of HIPAA data security standards mandates that security risk assessments must be performed periodically, safeguards must be implemented under the security rule during patient data exchanges, and security breaches must be reported to include data loss of control through ransomware encryption.

Health Information Technology for Economic and Clinical Health

Furthering the support of HIPAA compliance, HITECH is Title XIII of the American Recovery and Reinvestment Act (ARRA) and provides a considerable focus on data breach reporting requirements and enforces compliance through criminal and civil penalties (Mariani et al., 2015). Mariani et al. (2015) elaborates that the reporting requirements outlined in HITECH compel organizations to report security breaches within 60 days of the incident, notify local news of affected individuals of 500 or more, and report breaches involving PHI to the U.S. Department of Health and Human Services. The author informs that IT security managers may find challenges in optimizing HIPAA and HITECH effectiveness considering the demands of increased funding and manpower to implement the standards. The author concludes by recommending that IT security managers of health organizations should promote and cultivate a security vigilant and conscientious organizational culture. HITECH also is primarily contributive to the widespread practice of the "meaningful use" construct and the wide adoption of EHRs through targeted financial incentives which raised by 83.2% between 2009 and 2014 (Johnson & Kwon, 2015). Each of the mentioned healthcare-related frameworks, standards, and associated theories complements the PMT by managing associated risks of data traversing IT systems common and particular to the healthcare industry least fear of compromise.

Healthcare Information Technology and Security Challenges

To fully grasp the significance of the fundamental challenges IT security professionals face concerning managing inherent risks associated with interconnected

healthcare systems and services, it is essential to understand the importance of IT facilitated data and information sharing platforms about healthcare-oriented processes. The healthcare industry has been dramatically transformed concerning its adoption of information technology which has facilitated positive change through automated business processes, enhanced health information sharing, considerably accelerated data processing, and improved overall health organization performance through IT strategic alignment (Alsharif et al., 2018). Clinical information systems and medical IT solutions are increasingly becoming an essential strategic need, considering the readiness of healthcare organizations (Haddad et al., 2017). IT-based medical devices, workstations, and interconnected systems of today are progressively using and sharing network resources globally. This effort has resulted in government incentives and created an environment of technological advancements and interoperability for medical centers and hospitals to support the myriad of medically-oriented functions necessary in the healthcare field (Keenan et al., 2016).

However, there is considerable complexity to the implementation, management, and maintenance of healthcare IT systems, but more importantly, is the high degree of unintentional risks and consequences to medical networks regarding data and information sharing (Lee, 2017). When considering some of the prominent vulnerabilities related to interconnected healthcare systems, there are varied areas in hospitals that are more susceptible to the threat of data breach than others. In this regard, some IT security managers use multivariate logistic regression analysis as a method of comparing variables by which the hospital characteristics are explored to influence predictive factors

of a data breaches that affect no less than 500 patients (Cortelyou-Ward et al., 2018; Liu L., 2018). Distinctively, there have been sharp increases regarding breaches in data security and PHI, which are becoming a dooming reality for health organizations. Government health organizations of the United States have experienced breach increases in upwards of 70% between the years of 2010 and 2017 and 27 VA hospitals suffered data security breaches in less than 10 years (Cortelyou-Ward et al., 2018).

Lo et al. (2018) states that there has been at least $7 billion worth of annual losses related to breaches in information security within the healthcare industry. Lo et al. (2018) concluded that patient perceptions are correlated to patient trust and is supplemented by organizational investment in data protection mechanisms which attest to positive cyber safety procedures, policies, and practices reflective of institutional trust. Further analysis of the human-factor regarding security breaches reveals that information security education of health information systems has been one of the principal approaches to mitigating associated risks (Arain, Birney, Hepp, & Tarraf, 2017). Arain et al. (2017) investigated information security training and education of employees in health organizations using semi-structured interviews and focus groups and found a correlation between security breaches to IT security programs. Security vulnerabilities signify significant differences in staff perceptions and experiences as they relate to security awareness and effectiveness remedied by empowering employees with sufficient knowledge of secure practices under a communally policed environment (Arain et al., 2017). Thompson and Zandona (2017) communicate how cybersecurity initiatives have mostly been incremental and rarely have been transformational about providing a

relevant strategy based on the analysis of supporting literature regarding health cybersecurity. Methods to address cyber-threats are strategic combinations focused on both the technical and non-technical initiatives and organizational culture change to defend and safeguard health information (Thompson & Zandona, 2017). Arain et al., 2017; Lo et al., 2018; Thompson and Zandona, 2017 research provides analysis supporting functions of human-factors within an organization to further develop a strategic baseline and associated objectives, addressing approaches to cybersecurity in health organizations.

The use of mobile technologies in or supporting health organizations has also been a growing concern concerning the security of patient data. Jalali and Kaiser (2018) address the issue of incidents within the cybersecurity domain, which have steeply increased regarding the threats associated with health organizations in general and hospitals specifically. The authors focus on how the healthcare industry has struggled in comparison to other industries in protecting patient data, and the investment hospitals are now recommended to make regarding systems protection. Jalali and Kaiser (2018) also recognize and discuss the fact that some hospitals faced challenges with maintaining technology, increased technological complexity, inner-politics, and regulatory demands as obstructions to progress. The purpose of the Jalali and Kaiser (2018) study was to develop a methodical and structural assessment for examining the development of cybersecurity in hospitals and hospital cybersecurity systems interaction in the United States. Medical information accessed through mobile technologies in support of medical institutions has not been immune to data breaches. To this point, Markelj and Vrhovec

(2018) also center their research on the use of mobile technologies in the healthcare industry as an important part of the critical infrastructure within information security management. The purpose of their research is to evaluate the relationships between mobile device use, following hospital information security standards and policies, and data breach consequences. Their research focused on access to medical data through the use of personal and work mobile devices. The study resulted in a perceived element of personal consequence that is negatively related to personal and work mobile devices used for medical data access applications (Markelj & Vrhovec, 2018). Both the Jalali and Kaiser (2018) and the Markelj and Vrhovec (2018) studies highlighted that to fully understand effective data breach prevention techniques, an information security manager within the government health organization should review the internal and external IT risks mobile technologies present.

There is a strong correlation between observing information security standards and policies and the consequences of data breaches for both the hospital and its patients. Chen et al. (2017) performed analysis and outlined some of the development problems regarding the framework of processing information and how information is constructed related to information security management in hospitals. The methods used to develop the study were facilitated by a network-based questionnaire to analyze various levels of compliance about general hospitals in different locations (Chen et al., 2017). The results provided adequate data to conclude that the construction and prudent management of hospital risk and information, advances and enhances the secure collaboration of interconnected platforms and network security management (Chen et al., 2017). Sadoughi

and Zarei (2016) references the risks to information security and providing adequate structured approaches to information security risk management in line to prevent breaches. Similarly, the foundation of the Kim et al. (2018) study details the exploration of evidence that supports a clear path to understanding how medical institutions have improved information security risk management over 10 years. The Chen et al. (2017), Kim et al. (2018), and Sadoughi and Zarei (2016) studies focus their research on health organizations that have made efforts to improve information protection levels and information security postures by establishing both countermeasures and administrative measures specifically to physical and technical security.

Information Technology Risk Management: Preparation and Categorization

Organizational-Level Preparation

In terms of preparing IT systems and controls for integration, some organizations use the preparation phase to center on the activities that may be conducted in the organization that is critical to preparing the organization for risk management adoption. The preparation phase can include assigning appropriate roles and responsibilities, understanding the mission, associated threats and risk tolerance level, and the key stakeholders of the organization (NISTJTF, 2018). Also included in the preparation phase is prioritizing assets, conducting risk assessments, prioritizing security requirements, understanding the overall enterprise IT environment, understanding authorization boundaries for both IT systems and controls, and developing controls appropriate for the associated IT system (Ammenwerth & Leber, 2017; NISTJTF, 2018). In this preparation-based phase, the objective is to set priorities for security and privacy management as they

relate to the organization. Johnson et al. (2016) concluded, in a study of information management trends, that cybersecurity is of the top three growing concerns in U.S.-based organizations, which emphasizes that senior leaders identify and assign roles accordingly to balance strategic and operational responsibilities. The authors in the study elaborated on the roles, responsibilities, and chief information officer (CIO) reporting relationships between other IT professionals as they relate to risk mitigation practices, cybersecurity, and risk management strategy. Understanding key roles are particularly key to adopting a risk management structure. Although the terminology varies depending on the various frameworks, standards, or structures, common roles are authorizing official (who assumes responsibility and accountability of organizational systems operation) and the chief acquisition officer (who serves as the advisor to the organization lead on mission fulfillment and acquisition activities) (Karanja, 2017; NISTJTF, 2018). Also, fundamental to risk management is the role of the CIO or enterprise architect who is overall responsible for the implementation and integration of the enterprise architecture and its components, maintaining information security platforms, policies, procedures, and stakeholder coordination and collaboration of information requirements (Karanja, 2017). Some other key roles are common control providers and assessors responsible for implementing, assessing, monitoring controls, and the risk executive who provides an extensive enterprise-level methodology to risk management (Alexander & Cummings, 2016; NISTJTF, 2018). The relevance of this research reflects the preparation phase of adopting risk management practices, which demands well-defined roles and responsibilities before adoption.

Another key element to adopting and integrating risk management functions is understanding organizational risks through the performance of the organizational risk assessment when preparing the organization for management risks (NISTJTF, 2018). Cagliano et al. (2015) describes the risk management process, which enables risk management strategy development as the objectives, methods, and supporting resources used to facilitate risk activities considering organizational risk maturity and tailored control baselines. There is an emphatic need for organizations to periodically assess risk and control risk (Biskupek, 2018). Kwong et al. (2016) explored the importance of conducting initial and periodic risk assessments to understand risks related to people, processes, and products, and conclude that IT risks primarily originate from vulnerabilities associated with people-related risks. Javani and Rwelamila (2016) expand on risk process development stating that the risk assessment, which is divided into risk analysis and risk prioritization, follows risk identification and is statistically more often focused on qualitative risk over quantitative. Identifying and analyzing risks of the organization leads to adopting specialized control sets developed for organization-wide use, directed by requirements engineering (Emmerich et al., 2016). Organizationally-shaped control baselines are paramount to IT security managers regarding the overall security posture of an organization and addressing specific organizational privacy risks (Cenys et al., 2019). In their study of defining security baselines, Cenys et al. (2019) states that organizations could facilitate cost-effective and required levels of protection through the implementation of organization-tailored minimum security control baselines. Understanding the mandatory requirements of standard security controls of a government

health organization is relevant to this study detailing the establishment of organizationally-tailored control baselines and enabling common controls for organization preparation outlined in common risk management methodologies.

System-Level Preparation

Similar to the organization level of risk management preparation, the management of processes and procedures is central to preparing organizational systems for the adoption of the framework. Primary tasks associated with initiating risk management preparation at the system level are verifying business alignment, stakeholder management, identification of assets and defining requirements, understanding the system types and the system lifecycle, and determining the authorization boundaries (NISTJTF, 2018). System-level preparation is designed to prepare the organizational IT infrastructure supporting functions for the IT system and associated adoption of controls in terms of identifying key tasks, understanding primary roles, and integrating supporting roles.

Freitas et al. (2018) stated that it is critical to the successful management process to set performance indicators that represent IT system alignment with business priorities and objectives and adopting an agile methodology for both flexibility and adaptability. The authors emphasize organizational success management processes as they relate to implementing IT systems, working through the associated complexities, and employing systematic processes for IT project management improvement and deliverables performance. Their study concluded with a path to codifying processes to identify and define the criteria and milestones essential for assessing IT project critical success factors

for business mission alignment. The element of aligning the IT system with the business mission focus of a government health organization is a fundamental success management process and is a supported task in most risk-based frameworks that identify business processes satisfied by the IT system.

Organizations should consider system stakeholders who are identified as those individuals internal or external to the organization that has vested interests in the system life cycle for its development, design, delivery, implementation, operation, and sustainment of the organizational systems (NISTJTF, 2018). Ahriz et al. (2017) stated that IT system alignment with organizational strategy is a result facilitated by the integration of stakeholders in the project lifecycle early in the processes of periodic risk management assessment and risk mitigation. The authors' objective of the study was to highlight the disparities between IT practitioners and IT researchers in a professional environment concerning primary supporting methodologies, frameworks, and techniques of IT project risk management. The study concluded with the focus on the synergic implications stemming from best practices modeling the integration of governance frameworks for greater inclination toward adoption, increased efficiency, and IT strategic project alignment. The factors of stakeholder involvement at the early stages are significant to facilitate initial and continual stakeholder communication consistent with industry best practices to meet security and privacy requirements. Stakeholder involvement and communication also support alignment with strategic IT governance and IT project management models throughout the SDLC.

The combination of both tangible (physical/ environmental) and intangible (not physical), assets make up the total assets of an organization that needs to be identified, prioritized, and protected accordingly (NISTJTF, 2018). Identifying assets of the organization comprise of tasks that traverse all three organizational levels of strategic, operational, and tactical and is an initial step to understanding and protecting the privacy posture of the organization and stakeholder interests. Almeida et al. (2018) state that information over time has developed into the most valued asset of an organization and, respectively, has been the target to a succession of progressive threats via exploited information security vulnerabilities cultivated by a general lack of asset identification and security control management. Almeida et al. (2018) highlight some significant challenges faced by small to medium-sized enterprises in terms of security policy development, and they outline asset management, security risk management, scope, and other supporting elements as key components of security policy. Particular to the conclusion of the study is the identification of information assets that must be protected as they pertain to risk management and therefore considered within the development of the security policy. The identification of organizational information assets plays a vital role in assessing authorization boundaries and subsequently helping information security managers understand various types of information within those boundaries. The identification also contributes to defining the applicable information security requirements reflective of the information life cycle and risk assessment within several types of risk and cyber security-based frameworks (Ammenwerth & Leber, 2017; Belaissaoui & Elkhannoubi, 2015; Jalali & Kaiser, 2018; Retnowardhani & Yoseviano, 2018).

The advent of an interconnected world brought on by such concepts as globalization, and the internet of things (IoT) platform integration has made electronic commerce, information sharing, and information processing borderless operations. Data traverses locally, regionally, nationally, and internationally in open exchange digital environments throughout the world (Baldi et al., 2019). This paradigm expresses the requirement to define authorization boundaries, which denote the organizational limits of the authorized scope of system accountability and protection (Considine et al., 2019). Aljohani et al. (2018) states data and information security managers in the healthcare industry have seen new cybersecurity challenges with securing private data considering the integration of bioengineering communication platforms such as body area networks and wireless sensor networks. Aljohani et al. (2018) evaluated the security posture of networks that have integrated wireless body area network technologies. Kim et al. (2018) also explored the integration of practical security assessments to implement security measures that help identify and prevent network attacks. Considine et al. (2019) and Aljohani et al. (2018) highlight the importance of defining general authorization boundaries that information security managers should consider, which may be specific to the healthcare industry about provisioning for security controls.

Significant to the preparation phase of most risk-based methodologies, is identifying, categorizing, and protecting various types of information within the authorization boundaries of government health organizations. Such identification and classification of various data and information types within cybersecurity and risk management constructs signify the relevance to the mission and business functions of the

organization and the potential of risk if a compromise is realized (NISTJTF, 2018). Baldini et al. (2019) states that security labels are fundamental tools used to identify sensitive data and information to ensure regulatory compliance, prevent leaks of PII and PHI, facilitate accurate reporting of data loss, positively influence governance and user accountability, and streamline encryption. Baldini et al. (2019) outlined statistics of data and information breaches and data leaks throughout the world. Baldini et al. (2019) also focused on codifying the benefits of facilitating data classifications techniques as a prevention method. Identification and classification of the information types hold specific relevance to dealing with risks by addressing the methods at the system level by which a government health organization may administer controls comparable to elements of risk associated with information processed, stored, and transmitted within the information life cycle (Baldini et al., 2019; Collard et al., 2017; NIST, 2004; NISTJTF, 2018). Information security managers may benefit from a developed understanding of information types and their interrelationships that correlate to organizational risks (Baldini et al., 2019; Chen et al., 2017; Collard et al., 2017; NIST, 2010; NISTJTF, 2018).

Preparing a government health organization to adopt effective cyber risk management processes, similar to any other organization and industry, will require an assessment of relevant risks as they pertain to a given system or system implementation and the likelihood of realized threat impacts (Boonjing & Pimchangthong, 2017; Fugini et al., 2016; Gan et al., 2020; Keenan et al., 2016). The security of systems within a government health organization may be dependent upon a thorough risk assessment, the

analysis of the associated outcomes, and the risk relevance to the organization and its stakeholders (Ammenwerth & Leber, 2017; Belaissaoui & Elkhannoubi, 2015; Jalali & Kaiser, 2018; Retnowardhani & Yoseviano, 2018). Historically, a risk evaluation innately focused on the security triad: confidentiality, integrity, and availability of the information system established in the organizational systems architecture (Baldi et al., 2019; Kwong et al., 2016). Evolutionary accounts of the risk assessment concepts based on three stages consisting of computer security research development, system information security, and information infrastructure security (Baldi et al., 2019; Kwong et al., 2016; Nan et al., 2016). Nan et al. (2016) expounded that the computer security research and development stage mostly followed computer security theory research and Department of Defense (DoD) guidelines. The research of Baldi et al. (2019), Kwong et al. (2016) and Nan et al. (2016) concluded on promoting the use of the incremental factor analysis methods, which divides information systems security into risk parts and systematically assesses each risk part, which inherently accounts for information systems expansion. Some IT security managers will find an added benefit in this regard to codify methods of evaluating risk at each relevant risk stage. Subsequently, the need for information security form a systems perspective and mostly center on the development of commercial computer security models and standards ground in systems security. Finally, compounded research and development throughout the years focused on information security as an infrastructure, accounting for enterprise-level concepts and the protection of information systems throughout the organization. The Baldi et al. (2019), Kwong et al. (2016) and Nan et al. (2016) research is relevant to conducting thorough risk assessments by accounting for the

growth of information systems architecture and how that growth inherently increases the amount of risk assessed. The architectural growth to increase in risk ratio may be a significant concern for some government health organizations.

The potential inputs leading up conducting the risk assessment are understanding the mission or purpose and processes of the organization, its protected assets, and potential stakeholder and system threats and threat impacts (Ellingson et al., 2017; Frederick et al., 2017). Also, the system design and overall system architecture, overall risk management strategy, and the cybersecurity framework may play a vital role in conducting accurate and detailed risk assessments (NISTJTF, 2018). Anderson and Manson (2019) affirm that IT security managers conduct risk assessments to identify and prioritize risks and understand cybersecurity vulnerabilities achieved through the analysis of accurately documented diagrams such as Purdue (simplified network architecture), physical architecture (equipment and connections), and data-flow diagrams (communications on the network). Ellingson et al. (2017), Frederick et al. (2017), and NISTJTF (2018) focus on the premise of IT security professionals following best practice practical design principles that adhere to more comprehensive protection and control of systems. The research of Ellingson et al. (2017), Frederick et al. (2017), and NISTJTF (2018) concludes with cybersecurity recommendations of consistent defense-in-depth application, organizational culture-based adoption of the cybersecurity program, network sectioning, and data diode use for manageability, detailed risk assessment, use of data movement documentation, and the use of embedded watchdogs throughout the network. The Ellingson et al. (2017), Frederick et al. (2017), and NISTJTF (2018)

recommendations hold significance for the preparation of organizational cyber risk management adoption by addressing solutions to common adoption failures or problems.

Baldi et al. (2019) asserts that integral to maintaining a comprehensive cybersecurity program is the integration of risk assessment and risk treatment processes to ensure that security controls sufficiently establish the appropriate level of cyber threats response. Ellingson et al. (2017) and Frederick et al. (2017), explored the various methodologies which contribute to understanding cyber threats through several risk assessment processes, which supplement some of the fallacies inherent with the sole selection of qualitative or quantitative approaches. Ellingson et al. (2017), Frederick et al. (2017), and Baldi et al. (2019) suggests the use of aggregated source data, which culminate in a quantitative-based methodology detailing generalized potential annual tangible and intangible loss from cyber risk exposure. The research of Ellingson et al. (2017), Frederick et al. (2017), and Baldi et al. (2019) has significant relevance regarding the preparation of government health organizations for cyber risk management adoption by specifying how combinations of both qualitative and quantitative methods of risk assessment can be uniquely combined and integrated to provide security managers overall comprehensive risk awareness.

Information security managers develop greater insight into defining privacy and security-based requirements at system levels after the risk assessment. System security and privacy requirements are essential considerations that play a vital role in the reduction of risk to an acceptable level, inform security controls selection and customization, and support business objectives, mission advocation, and stakeholder

engagements (NISTJTF, 2018). Rezaeibagha et al. (2015) state that simultaneously providing health systems protection and health services interoperability is dependant upon identification of security and privacy requirements through the implementation of U.S. standards such as HIPPA, Health Information Technology for Economic and Clinical Health Act (HITECH), and Health Level Seven (HL7). Rezaeibagha et al. (2015) highlight various methods of identifying requirements for protection and privacy for data processed through health systems through a detailed literature review. Moreover, the authors address health system data exchange privacy and security requirements through concepts of access control, secure communications, security standards compliance, and enabling interoperability. Rezaeibagha et al. (2015) concluded with the emphasis on the adoption of industry standards and well-defined access control policies, which is significant to the secure operational environment of government health organizations regarding the exploration of identifying security and privacy requirements. The system security and privacy requirements, which comprise the overall security and privacy architecture, ensure alignment between organizational systems and the risk management strategy (Rezaeibagha et al., 2015). Moreover, the identification of security and privacy requirements within government health organizations facilitate the proper allocation of resources and requirements through the organization, therefore informing and influencing organizational control selection and implementation.

Security and privacy architectures are important parts of the overall enterprise architecture. The enterprise architecture, as it relates to the preparatory phase of the risk management, builds on the foundation of system placement within the enterprise and

outlines the interconnectivity between systems within and external to the organization (NISTJTF, 2018). The enterprise architecture also denotes the establishment and relationship between security domains. Moeini and Rivard (2019), Retnowardhani and Yoseviano (2018), and Vinnakota, (2016) conceptualized that as technology advances, so too does cyber risk and subsequently calls for a revolution in the way enterprise executives, information security managers, and other cyber professionals explore cybersecurity governance for the multidisciplinary complexities consistent with most enterprises. Vinnakota (2016) promoted the implementation of the cybernetic model, which influences enterprise executive staffs and cybersecurity managers to focus on: *why*, *what*, and *how* of cyber governance. Vinnakota (2016) described seven elements of the cybernetic model as strategic direction development, cybersecurity performance measurements, cyber-environment scanning, collaboration and strategic initiatives, evaluation of future cyber threats, strategy modeling, and the selection and implementation of cybersecurity strategy. Lü, Wang, Xu, and Zhang (2019) and Vinnakota (2016) also noted that the seven elements of cybernetic model strategy development more adequately address the "*why*" as the interests of the enterprise and its shareholders, the cybersecurity vision and risk management of the enterprise as the "*what*", and the "*how*" as the development of cybersecurity policies, decisions, and cybersecurity program management. Models such as the cybernetic model intrinsically facilitate effective communication between executive-level staff and cybersecurity professionals and influence greater communication between risk management processes and executive-level governance within the enterprise (Lü et al., 2019; Moeini & Rivard,

2019; Retnowardhani & Yoseviano, 2018; Vinnakota, 2016). These considerations are major objectives in cyber risk management system preparation and significant to the risk management processes and communication, which lead to system registration within the government health organization (NISTJTF, 2018).

Categorize the System and System Information

Government health organizations have experienced significant information security breaches over time as the technological infrastructure of many government hospitals, clinics, and other healthcare institutions have expanded, and IT system dependency has increased. Challenges faced by some cybersecurity professionals in the healthcare industry are gaining an in-depth understanding of the needs of each authorized IT system and eHealth system and the various types of data and information that require access and must traverse the networks of the organization. The categorization tasks within cyber risk management influence both accountability and impact of loss analysis and specify the categorization of systems within the organizational architecture in terms of asset management and the information processed, stored, and transmitted throughout the information lifecycle (NISTJTF, 2018). According to NIST (2004), the categorization of U.S. federal government information and information systems is defined by potential impact to organizations regarding the security objectives of the security triad. The potential impact is low when the loss of any or all security triad members have limited adverse effects, moderate when a loss is considered serious, and high when a loss is considered catastrophic to the privacy and security of the organization (NIST, 2004).

Categorization begins with a detailed system description and documenting the characteristics of the information system accordingly (NISTJTF, 2018). Some of the descriptive language and criteria used to describe and document information system characteristics are the use of a descriptive system name (Ammenwerth & Leber, 2017; Belaissaoui & Elkhannoubi, 2015; Cao et al., 2019; Du et al., 2018). Bartol et al. (2018) emphasizes the necessity of documenting detailed system characteristics and prioritizing systems, programs, and components based on their significance to the mission of the organization and the risk they present to the organization if loss realized. Bartol et al. (2018) use the criticality analysis process model as an organized and controlled method of helping IT security managers understand information systems in detail, their contribution to the organization, and the risk of loss (Bartol et al., 2018). The criticality analysis process model and similar analytical models, detail system design and implementation relevant to the organizational mission and consists of five processes of defining system criticality procedure within the organization, program-level criticality analysis, system and subsystem-level criticality analysis, component and subcomponent-level criticality analysis, and review of criticality processes (Ammenwerth & Leber, 2017; Bartol et al., 2018; Belaissaoui & Elkhannoubi, 2015; Cao et al., 2019; Du et al., 2018).

Most IT security managers of government health organizations will gain greater benefits by meticulously describing the programs, systems, subsystems, components, and subcomponents of the organization when using the criticality analysis process model (Bartol et al., 2018). The descriptions can include identifying information such as the

system name, ID or serial number, version number, manufacturer information, persons accountable or responsible, physical and logical location within the architecture, contact information, purpose or business function, and authorization and governance information (NISTJTF, 2018). Descriptive information can also include how data and information flow through the system (Bailey et al., 2011). Models such as the criticality analysis process model are significant to government health organizations to logically define systems and systems of systems in terms of their design, acquisition, and implementation throughout the organization. Moreover, the model is a mechanism used by IT security managers to gain a holistic view of system criticality by using both a top-down and bottom-up approach progressively narrowing analysis down to critical systems through reviewing critical processes and focusing on the point of realized risk or loss up to the larger system to analyze greater impacts respectively (Bartol et al., 2018; Lee, 2017; Sadoughi & Zarei, 2016).

Kim et al. (2018) proposed an improved weighted machine learning method using the LeaderRank algorithm for the identification and categorization of critical systems, and it's components as a precursor to predicting and analyzing the application of controls and system reliability. The authors used a common node (ground node), its associated reverse connections, and the weighted context of the adjoining nodes to the ground node to provide a directional path of ordering nodes by criticality within the network architecture of the organization. This technique provided an improved method of understanding system importance as it relates to the organizational system and network architecture (Cao et al., 2019). Lü et al. (2019) used the SpectralRank machine learning

algorithm within complex organizational networks to predict the propagation capabilities of network nodes. The authors consider the SpectralRank algorithm to be more accurate than LeaderRank about gaining an understanding of complex uncorrelated networks. This algorithm also uses a ground node as the foundational node from which the characteristics of the connected node are derived (Lü et al., 2019). Both the LeaderRank and the SpectralRank machine learning algorithms are relevant to the categorization common in most risk management schemas as methods of providing system-based descriptive information for IT security managers to understand their level of importance to the mission of the organization and influence relevant planning for system controls.

Common objectives in cyber risk management highlight the requirement to categorize information that flows through the system relative to providing a complete security picture of the systems in the organization (NISTJTF, 2018). Collard et al. (2017) states that a prominent definition of security classification is the categorization of information and information systems in terms of criticality to the mission of the organization and reference to governing factors such as laws, standards, guidelines, organizational policies, and regulations. Collard et al. (2017), Ellingson et al. (2017), and Frederick et al. (2017) further defines security classification from the perspective of IT security professionals as categorization to aid the protection of threat impacts and the consideration of inherent information-based risk, information owner risk, information storage risk, and legal risk. Collard et al. (2017), Jalali and Kaiser (2018), and Retnowardhani and Yoseviano (2018) sought to update and more accurately define information security classification using the categorization of organizational assets:

information and information systems. The categorization of information is a well-known and necessary process to help IT security managers identify and document intangible information system critical assets and is also a significant process in gaining a deeper understanding of what to protect and how to protect it based on its criticality. After the systems and associated information is identified and categorized appropriately, an authorizing official conducts a review and approval of the proposed categories of the systems, systems of systems, and the information processed within the organization (Boonjing & Pimchangthong, 2017; Javani & Rwelamila, 2016; NISTJTF, 2018).

Information Technology Security: Security Controls

Select Security Controls

Following the preparation of the organization for cyber risk management adoption and appropriately classifying and categorizing systems and information within the organization, the planning processes migrate toward selecting the appropriate security controls. In this step, themes within the literature that supported the risk-based control selection processes were centered on controls implementation, the system categorization, and the results of the risk assessment. Equally supported were the overall risk management strategy, system security, privacy, and contractual requirements, and the analysis of business threat impacts and analysis of system criticality can all be used as inputs. NIST (2013) defines and categorizes security control structure into 18 families which help determine criteria that affect the controls such as policy, supervision, actions of individuals, manual and automated processes, and oversight.

The Center for Internet Security (CIS) (2019) furthers the NIST-based family of controls with 20 recommendations of the most common security controls based on cybersecurity industry best practices. The 7.1 revision of the CIS security controls is categorized into 3 pertinent implementation groups that are defined as basic, foundational, and organizational CIS controls (Center for Internet Security, 2019). The premise behind the basic CIS controls is conducting hardware and software inventories, vulnerability and administrative privilege management, mobile device and workstation security configurations, and continuous analysis (Center for Internet Security, 2019). The foundational implementation of security controls facilitate email and web security, malware and boundary defense, ports, protocols, and services security, and wireless, account, physical, and data access control and protection (Center for Internet Security, 2019). Lastly, the Center for Internet Security (2019) addresses security awareness and training, application security, incident response management, and penetration testing within the organizational CIS controls construct. The 20 security controls that CIS recommends detail key aspects of security that most IT security managers within government health organizations will find it beneficial to achieve a viable security baseline.

Baseline (pre-defined) and organization-generated (specialized) are two options for the selection of controls (NISTJTF, 2018). Both options ultimately assist information security managers of government health organizations in selecting relevant security controls for the systems of the organization while considering the operational environment. Rotella (2018) emphasizes the importance of security baselines, stating that

measuring the success of security controls in terms of managing system vulnerabilities is not reliably feasible without control baselines and internal benchmarks. The author states that security control baselines enable the reduction of vulnerabilities, the identification of positive engineering practices and processes, and the improvement of methods to circulate the best security development lifecycle practices (Rotella, 2018). Rotella (2018) concluded that the security control baselines of the organization aid IT security managers by providing a point of reference for vulnerability management within the organization, and without this reference, security engineers are challenged in providing effective security measures. However, not only are security managers faced with challenges, decision-makers such as senior-level management and executives are challenged in making prudent and informed decisions that pertain to control selection. Emmerich et al. (2016) states that the selection of security controls has traditionally been a two-stage decision-making process consisting of defining the size of the security budget and the subsequent action of budget distribution among assorted and relevant security controls as an information security officer responsibility. However, the authors emphasize an adopted perspective informed by the information security manager to view security control selection through relative and unaltered organizational baselines as a method of providing a more accurate and realistic interpretation of security control effectiveness.

Emmerich et al. (2016), NIST (2018), and Rotella (2018) conclude that the process of quadratic programming enables IT security managers to view loss prevention through baselined or organic system security controls as a measurement of gains and solving the problems of budget constraints and unproportionate risk and return balance.

This proposed solution can benefit government health organizations in security control selection by emphasizing the minimization of threat probability and potential losses and quantifying the value of security investments, thereby strengthening executive staff commitments to the security budget. It is well understood in many IT security manager circles that the key to having and maintaining a respectable IT security budget is having the buy-in of organizational decision-makers. After this, the selection processes depend on the supporting criteria of the system protected and the protection method or methods used.

Nikishova and Vitenburg (2019) state that system security controls selection is dependent upon the protected system or systems, the placement within the enterprise, and the information protection resource and its components. Nikishova and Vitenburg (2019) express the benefits of using statistical-comparative analysis of system attack vectors and subsequently assigning threats to threat categories relative to the organization as a method of initializing the selection and allocation processes of information protection systems and cybersecurity resources. Nikishova and Vitenburg (2019) also suggest that system security control selection methods can be supplemented for the sake of greater efficiency through the automated processes using a neural network (multilayer perceptron) to compare statistics provided from threat category analysis. Abraham et al. (2019), Ahmed et al. (2019), Diehl et al. (2016), and Frederick et al. (2017) proposed similar methods which enable IT security managers of government health organizations to compare and contrast the statistics surrounding probable threats and threat vectors to the organization through neural network processes. The comparative processes ultimately

aid in the selection and application of security controls and supporting information protection systems. The outcome of the proposed methodology is designed to supplement the human-factor, ultimately increase security controls selection efficiency (Abraham et al., 2019; Ahmed et al., 2019; Diehl et al., 2016; Frederick et al., 2017; Nikishova & Vitenburg, 2019).

Small and Wainwright (2018) and Birkinshaw et al. (2019) outline the selection of automated intrusion detection and prevention system (IDPS) controls based on continuously being able to monitor a network for abnormal activities, detect malicious network-based traffic, and the capability to implement relevant countermeasures against cyber-attacks. Birkinshaw et al. (2019) researched their model of IDPS using software-defined networking (SDN) grounded on the OpenFlow protocol. Both authors, Small and Wainwright (2018) and Birkinshaw et al. (2019), concluded that certain elements of SDN-based IDPS can successfully detect scanning attacks based on flow statistics and protect against denial of service (DOS) attacks affecting platforms that use TCP, UDP, and ICMP protocols.

However, some situations warrant organizations to use baselines as a platform to ultimately tailor an information security system control measure. Some selection methods do not fit a “one size fits all” model and require selection considerations with the intention of customizing protection systems and resources to fit into the cybersecurity strategy of the organization. As an example, Fuchs et al. (2016) and Small and Wainwright (2018) underlined the selection processes that led to the migration from paper-based medical records to EHRs as a dynamic that yielded increased complexity for

provisioning healthcare information protection measures. The complexity of provisioning for access control, risk management, and enabling sustainable workflow processes influenced security managers to adopt an organization-tailored or multi-methodology approach (Abercrombie et al., 2017; Alsharif et al., 2018; Emmerich et al., 2016; Fuchs et al., 2016; Small & Wainwright, 2018). This approach addressed the thematic challenges of selecting and tailoring an EHR platform suitable for various health organizations (Fuchs et al., 2016; Small & Wainwright, 2018). Alsharif et al. (2018), Abercrombie et al. (2017), and Emmerich et al. (2016) explored the various complexities of selecting and tailoring control systems. Fuchs et al. (2016), Keenan et al. (2016), and Small and Wainwright (2018) explored methods using case studies of successful multi-methodology applications in National Health Service (NHS) hospitals, relevant literature reviews, and several accounts of role-based access control application. Fuchs et al. (2016), NISTJTF (2018), and Small and Wainwright (2018) concluded that IT security controls multi-methodology described the identification of business strategies, objectives, and problem definitions used as inputs into the controls selection process and yields the output of relevant controls selection for the organization. The selection of controls will then be used by IT security and procurement managers as the input into the acquisition processes for strategic sourcing and implementation (Emmerich et al., 2016; NISTJTF, 2018). The IT security control multi-methodology is a platform that has the potential to help IT security managers of government health organizations systematically assist in the control selection process regarding the contextual adaption of problem structuring methods (Abercrombie et al., 2017; Alsharif et al., 2018; Emmerich et al., 2016; Fuchs et al.,

2016; Small & Wainwright, 2018). IT security managers should document planned control implementation and the monitoring strategy for the control systems (Fuchs et al., 2016; Kulkarni, 2019; NISTJTF, 2018). Also pertinent to control selection processes are the review and accompanying approval by an authorizing official of the implementation and monitoring plans which are commensurate with associated risks (Abercrombie et al., 2017; Alsharif et al., 2018; Emmerich et al., 2016; Fuchs et al., 2016; Kulkarni, 2019; NISTJTF, 2018).

Implement Security Controls

Literature themes of the implementation of security controls highlighted IT security managers implemented cybersecurity controls using best practices and mandatory configurations under the laws and regulations of the government and the strategies and policies of the organization. Diehl et al. (2016) and McEvilley, Oren, and Ross (2016) state that systems security is a product of systems trustworthiness considering the geographic and logical expansion, complexity, and dynamicity of systems and associated security controls. Systems security or cybersecurity engineering and implementation provide the architecture and design requirements needed to inherently make systems less vulnerable and more resilient to attack or degradation (Hillebrand, Karner, Rom, Romer, & Steger, 2016; McEvilley et al., 2016). Since cybersecurity is a consistently changing field, it is imperative to have a flexible strategy for security controls implementation to supplement evolving threats (Diehl et al., 2016; Emmerich et al., 2016; Hillebrand et al., 2016; McEvilley et al., 2016).

Belaissaoui and Elkhannoubi (2015) addressed cybersecurity implementation strategies by highlighting the need for IT security managers to implement cybersecurity controls under the considerations of implementing flexible and evolving technologies that reduce the organizational risks of system vulnerabilities and operational threats. Considering security control implementation, there is a need for IT, security managers, to integrate the key processes of availability management (to ensure information availability), IT service continuity management (to ensure information risk reduction and recovery), and incident management (to ensure minimal adverse impacts on the organization and the systems and services are restored quickly) (Belaissaoui & Elkhannoubi, 2015; Herath & Rao, 2009; Keenan et al., 2016; Monken et al., 2017). Such key processes emphasize the importance of the organizational, legal, and technological aspects concerning information systems implementation (Belaissaoui & Elkhannoubi, 2015; Herath & Rao, 2009; Keenan et al., 2016; Monken et al., 2017). The aforementioned key processes are relevant considerations for IT security managers in government health organizations as they relate to the implementation of cybersecurity controls and serve as fundamental aspects of effective cybersecurity and organizational strategy development. Likewise, Alam and Ibrahim (2019), Frederick et al. (2017), Jalali and Kaiser (2018), and Mariani et al. (2015) focused on cybersecurity pillars of technology (in reference to the rapid growth and development of technological resources such as big data, IoT, and cloud computing), people (outlining the role as cybersecurity implementors), and institutional (reflecting on the dynamic cybersecurity impacts of the interactions between stakeholders, communities, and organizations). The authors

concluded that cybersecurity must meet and overcome the challenges of cybercrime with comprehensive and comparative cybersecurity control implementation strategies that place emphasis on the pillars of technology, people, and institutions (Alam & Ibrahim, 2019; Frederick et al., 2017; Jalali & Kaiser, 2018; Mariani et al., 2015). These considerations are applicable to cybersecurity managers in government health organizations as they relate to the development of processes that enable information security implementation management and supports cybersecurity infrastructure development (Ahriz et al., 2017; Biskupek, 2018; Cagliano et al., 2015; Keenan et al., 2016; Moeini & Rivard, 2019).

Strawn and Vagoun (2015) state that robust cybersecurity controls implementation is a product of a strong control implementation research and development framework relating to the protection of government cyber-systems and the capability and flexibility of the control to quickly respond to cyberattacks. Cao et al. (2019) and Lü et al. (2019) explored cybersecurity control implementation through the use of algorithms, which reflected the awareness, adaptability, and reactive evolution to that of biological concepts like the immune system. The moving-target research implemented information security control systems are developed supporting the concept of specialized systems that detect and adapt to abnormal code or attacks and rapidly repair the information system architecture by patching vulnerabilities after eradication of the threat (Strawn & Vagoun, 2015). Cao et al. (2019), Lü et al. (2019), and Strawn and Vagoun (2015) concluded that the use of customized trustworthy spaces concerning implementing security controls ensures the support of a wide range of functional and

policy-based organizational security requirements within that space rather than researching security solutions that simultaneously meet all requirements possible. This concept may be explored for some IT security managers in government health organizations that are overly focused on implementing all-encompassing security controls to save resources and time of implementation. Once the IT security controls are implemented and engineered to reflect best practice methodologies of security and privacy plans, IT security managers can track and document changes to the planned and executed implementation of the controls within the architecture. Farrell (2016) asserts that change in cybersecurity architecture is a complex paradigm which requires an organization-wide change management life cycle to facilitate and integrate change elements that are both reviewed and approved by pertinent stakeholders.

Bailey et al. (2011) states that system change management uses the baseline system configurations, which represent a secure state as input from which changes are formally identified. Farrell (2016) elaborates that once identified changes are formally proposed and reviewed, the changes are then analyzed for any impact to the security of the organization, tested, approved by senior management, and implemented and documented by IT security managers. IT security managers use this process to facilitate system security and privacy integration requirements and to simplify security control change management concerning enterprise architecture (Bailey et al., 2011; Farrell, 2016). The change management process is facilitated by IT security managers within government health organizations as a pertinent aspect to the implementation of approved changes regarding the continually evolving nature of the security architecture (Abraham

et al., 2019; Ahmed et al., 2019; Bailey et al., 2011; Farrell, 2016). After the security controls are implemented along with any approved changes, the change management processes mandate an update in the security and privacy plans of the organization, and IT security managers then focus their efforts toward periodically assessing the security controls for consistent relevance to control organizational risks (Emmerich et al., 2016; NIST, 2018; NISTJTF, 2018).

Assess Security Controls

The prominent themes within this section of the literature review address the need to assess the security controls of the organization to understand if the controls are correctly implemented, operating as prescribed, and producing the necessary outcomes considering adherence to security and privacy requisites. Equally important is the need to select technically competent assessors (Clapper & Richmond, 2016). Assessment plans need to be provisioned, approved, and updated based on security and privacy strategies and business objectives, control assessments, and ensure reports are maximized through automation (NIST, 2010). Partial legitimacy of the security assessment program in the healthcare industry is dependent upon its adherence to general organizational governance under government laws, regulations, and organizational policies and objectives (Chen, Chou, & Yang, 2019). Authorizing officials of government health organizations may choose to either conduct a self-assessment of the security controls or procure services of an external organization or team to conduct impartial security assessments. IT security managers typically determine the methodology and metric boundaries used to verify

implemented controls are performing within the guidelines, standards, and policies of the organization.

Brilingaitė et al. (2019) affirm that advancements in the field of automated cybersecurity attack detection are not a comparable substitute for trained human cyber-defense professionals which serve as the principal defense of an organization. The authors researched the use of cybersecurity exercises by using a case study methodology of joint military and civilian cybersecurity exercises. The exercises were based on cybersecurity team assessments to determine the effectiveness and efficiency of the implemented security controls under stressed conditions from the perspective of a Blue team (cyber defenders) and the Red team (cyber offenders) (Brilingaitė et al., 2019). The authors concluded that the cybersecurity posture of an organization is strengthened with the employment of competent, self-developing, and team-oriented cybersecurity assessment teams. Anderson et al. (2015) explored cybersecurity team selection processes and cybersecurity team performance highlighting the myriad of human factor considerations enveloped in the selection of cyber defenders while addressing manpower and expertise gaps. The authors addressed cyber team selection, expertise, and manpower gaps by suggesting the acquisition of members with the highest propensity of becoming experts and members, which portrayed synergistic predispositions. Blair et al. (2019) states that the future of cyber defense is envisioned as multifaceted employment of multidisciplinary cybersecurity assessment teams that contribute diverse expertise in various cyber security-oriented fields of study. This paradigm is relevant to senior information security officers in government health organizations as a conceptual

framework which aid in the facilitation of the cybersecurity assessment personnel or assessment teams selection processes and the promotion of assessor independence and team synergy among a breadth of cyber assessment team expertise (Blair et al., 2019).

Security and privacy assessment plan integrated within the information security strategy of the organization help IT security managers assess implemented security controls for effectiveness according to the organizational strategic objectives (NISTJTF, 2018). For example, Jayanthi (2017) states that security control assessments are based on the critical infrastructure, business processes, technological infrastructure, applications, and business systems, people resources, and supporting information processing facilities such as data centers and disaster recovery facilities. Aljohani et al. (2018), Kim et al. (2018), Johnson and Kwon (2015), Rezaeibagha et al. (2015), and Small and Wainwright (2018) asserted that the security assessment would test the effectiveness of cybersecurity controls by identifying, analyzing and evaluating, and mitigating control vulnerabilities and employing informed and prudent cyber risk responses. Kim et al. (2018), Johnson and Kwon (2015), and Rezaeibagha et al. (2015) endorses the use of information security scorecards as a means to benchmark and evaluate implemented information security controls and map the alignment of information security objectives with business objectives relevant to the security assessment team. Karasev et al. (2016) states that security audits are planned to address the frequency of security assessments, the identification of responsible personnel and matching individuals to tasks, and the details of the audit processes.

One of the themes from the literature suggests that IT security managers should conduct various periodic assessments of security controls in the organization to determine the degree of effectiveness of the selected security controls and the correctness of the implementation. Baldini et al. (2019) stated that adopting a cybersecurity framework and certification methodology along with security assessment processes and standards will empower stakeholders to assess IT security infrastructure for enterprise-level IT and IoT deployments via automated processes. Baldini et al. (2019), Brilingaitė et al. (2019), and Gourisetti et al. (2019) focus on various security assessment techniques such as penetration testing (replicating possible attacks), fuzzing testing (transmitting valid and invalid messages to a system to determine causes for vulnerabilities), and regression testing (ensuring device updates do not alter system functionality). Baldini et al. (2019), Brilingaitė et al. (2019), and Nan et al. (2016) also focus on usage-based testing (meticulously testing the most used systems and components), risk-based security testing (uses security risk analysis as the premise of assessment), and code-based testing (detecting vulnerabilities in code). However, Aljohani et al. (2018), Brilingaitė et al. (2019), and Gourisetti et al. (2019) endorse the use of model-based testing (assessing a sample of systems in a natural environment) as their preferred method, proclaiming that model-based is a more cost-effective and efficient approach.

Themes derived from the literature proposes there are robust manual and automated systematic processes that can assess the three distinctive and prominent categories of IT security controls: physical, technical, and administrative. Most organizations process, handle and store data and information such as PHI and PII that are

sensitive to the organization itself or the individuals subject to the data management of the organization (Cohen et al., 2015; Hillebrand et al., 2016; Jurn et al., 2018). Several reviewed articles in this review express the requirements for security managers in government health organizations to address the security pillars of physical, technical, and administrative security controls (Abercrombie et al., 2017; Cohen et al., 2015; Hillebrand et al., 2016; Keenan et al., 2016; Liu, Zhang, & Zhu, 2016). Implementations of physical security controls are designed to protect data by placing security measures at the point of presence to both physically prevent and possibly deter unauthorized access to sensitive data management mediums (Abercrombie et al., 2017; Cohen et al., 2015; Hillebrand et al., 2016; Liu et al., 2016). There have been some strides made in terms of automated processes to ensure physical security measures are properly accessed for optimal placement and configuration within the organization. Various types of advanced automated assessments can be considered critical to security managers within government health organizations to understand gaps or vulnerabilities considering employed physical security measures (Baldini et al., 2019; Cohen et al., 2015; Jurn et al., 2018; Nikishova & Vitenburg, 2019).

Abercrombie et al. (2017) applies the cyberspace security econometric system (CES) approach tailored to a cyber-physical control system implementation to assess physical security controls using uses risk management processes to assess information permutations via a monetary valuation and relevant stakeholder engagement of each vector, dependency vectors, possible threats, and realized risk impacts of critical infrastructure. Then the security manager uses the assessment of physical security

controls calculation to assess the security privileges and access restrictions accordingly provided by implemented controls (Fusch et al., 2018). This approach focuses on and provisions for stakeholder engagement and enterprise-based inputs provided by a persistent schedule of security control assessments. Hillebrand et al. (2016) proposes using the security metrics of dependable embedded wireless infrastructure (DEWI) to provide analysis and insight into the effectiveness of cyber-physical systems and physical security controls. IT security managers can use system criticality to assess and support physical system parameters instead of using security levels (Hillebrand et al., 2016; Liu L., 2018). Security metric implementation is an iterative process that divides the system into manageable sub-systems and relevant components, weighs them by security level contribution to the overall security system, and each sub-system and component is assigned a predetermined value against its overall effectiveness (Abercrombie et al., 2017; Ahmed et al., 2019; Hillebrand et al., 2016; Liu L., 2018).

Liu et al. (2016) state that physical security efficiency is measured and defined by scheduled security assessments using a dependence model and dependence probability matrixes of EliMet which aid security managers to protect critical infrastructure networks (CIN). The EliMet hybrid security assessment framework uses the game-theoretic state-based model to assess physical security controls through an automated process that actively queries the system in a learning phase and employs calculated security measures to rate security controls effectiveness (Liu et al., 2016). The implementation of EliMet also minimizes the human factor by supplementing human interactions with automated processes to test physical security measures. Machine learning has been gaining

significant traction in recent years about employing auto-programmable neural network training algorithms to synthesize computational intelligence (Denning & Lewis, 2018). Cohen et al. (2015) proposes a reversal on the conventional approach using machine learning concerning physical security and red and blue team employment. The method of the authors focuses on the red team versus the natural migration to the employment of blue team tactics and implementations by using machine learning to analyze physical security sensors and systems for possible vulnerabilities for the red team attack (Cohen et al., 2015). The blue team or security manager then refine plans and policies accordingly within a set trackable number of dimensions within the problem space instead of the blue team or security manager defending against every possible attack vector (Cohen et al., 2015).

Implementations of technical security controls employ protective measures of the technological premise to defend against the exploitation of system vulnerabilities and unauthorized entry and exfiltration of data at data access points (Emmerich et al., 2016; NIST, 2013). Technical controls are implemented to protect data and information processed through the physical security infrastructure of an organization (Emmerich et al., 2016; NIST, 2013). An assessment of technical security controls usually investigates technologies such as encryption, authentication, an automated process of access controls, certificates, and file integrity (Cohen et al., 2015; Hillebrand et al., 2016; Jurn et al., 2018). Most security managers in government health organizations will assess the effectiveness of technical security controls through automated processes and various

other means (Abraham et al., 2019; Ahmed et al., 2019; Diehl et al., 2016; Frederick et al., 2017; Jalali & Kaiser, 2018; Mariani et al., 2015).

Davidoff (2017) asserts that security managers in organizations should test their technical security measures in place preferably through a disinterested third party which may employ external and internal penetration testing as a means to catch vulnerabilities outside the scope or view of internal audits. The author also emphasizes the commitment to implementing a widely used and accepted annual risk assessment to contribute to the development of a risk mitigation plan. Relevant to technical security controls, the author highlights that the risk assessment creates a clear pathway to assess the associated risk to technical security controls and aids in the development of a long-standing risk management plan and implementation of security controls. The overall objective of information security management systems is to preserve the security triad per organizational policies, guidelines, procedures, and adopted frameworks to increase accountability, improve information security performance, requirements substantiation, and support decision-making (International Organization for Standardization, 2016). Aldya et al. (2019) state that quantitative assessments or metrics can be used to analyze and improve the effectiveness of technical security controls by measuring and interpreting outcomes through mathematical and pragmatic approaches as detailed within the ISO/IEC 27004 information security metrics implementation standard.

Duan et al. (2017) addresses expected quality standards associated with the evaluation of security measures under five primary security criteria: revelation, secrecy, privacy, breakability; and abundance. Cybersecurity vulnerability assessments primarily

focus on analyzing systems, networks, and facilities through implemented organizational controls (Kwong et al., 2016). The practice of multi-criteria decision analysis (MCDA) aids in the development of prioritized criteria to address both the complexity and the inherent challenges faced by IT security managers to provide an accurate account of the organizational cybersecurity posture (Gourisetti et al., 2019). Most IT security managers within government health organizations will find benefit in identifying security baselines and performing, analyzing, and documenting technical information security assessments for the betterment of the overall security posture (Alaydrus et al., 2017; Duan et al., 2017; Gourisetti et al., 2019; Kwong et al., 2016). Fuchs et al. (2016) states that there are very few supportive means available for automated detection, improvement, and management of organizational IT security policies, which result in outdated or unadaptable policies, security vulnerabilities, and data management inefficiencies. Both Almeida et al. (2018) and Herath and Rao (2009) highlight that organizational security policies must change dynamically with the operational environment. Relative to IT security managers of government health organization and focusing on closing security policy management gaps, Almeida et al. (2018), Herath and Rao (2009), and Sadoughi and Zarei (2016) propose a dynamic policy management strategy structured around access and identity management environments that use key performance indicators (KPIs) and relevant user management data for automated policy discovery and fine-tuning.

Most government health organizations invest in employee security training and education programs to address an aspect of the human factor of IT security management as an administrative security control measure. Ellingson et al. (2017) affirms employee

information security training is an effective tool used by information security managers to prepare employees for elements of IT risk associated with relevant threats and the introduction of new technologies. Administrative control assessments also consist of cybersecurity control assessment reports which detail the output of each cybersecurity control measure in terms of effectiveness, risks, and recommendations for vulnerability mitigation (Kwong et al., 2016; NISTJTF, 2018). Assessment reports also present the opportunity to understand motives and methods of penetration testers or threat actors in the action of carrying out attacks to exploit vulnerabilities and the reports are documented for further analysis (Basile et al., 2017). Assessment reports should be used as input to planning and performing remedial actions to address inadequacies in implemented IT security controls (NIST, 2018). As an integral part of cybersecurity and cyber threat mitigation strategies, assessments should focus on end-to-end connectivity for thorough risk management (Monken et al., 2017). Relevant to IT security managers within government health institutions, assessment reports methodize the requirements to move forward with a mitigation plan and cybersecurity solution implementation.

Security managers should use completed security assessments and privacy assessments that detail deficiencies within the IT security architecture to conduct effective remediation activities that should be regularly reassessed (NISTJTF, 2018). Some security managers use automated vulnerability detection techniques to register, assess, and understand software vulnerability root issues and then implement automated vulnerability remediation techniques such as auto-patch generation to decrease organizational IT security risks (Jurn et al., 2018). Since there are inherent complexities

of both operational and economic dynamics that impact security remediation plans, Alshawish et al. (2019) suggests using an easy to understand, scalable, and a time-to-compromise (TTC) comparative security metric. The authors' proposal using TTC estimation focuses on remedial development from weighing the quantified output of relevant and pertinent IT security risks. This quantification is performed by generating a metric from a combination of network component interdependencies, adversarial skillsets, and the criteria of known and zero-day vulnerabilities that denote the potential time an adversary needs to exploit a system vulnerability (Alshawish et al., 2019). Building on security remedial action development, Hadar and Hassanzadeh (2019) states that planning and prioritizing remedial security actions are a product of relevant levels of risk and can be performed under agile security processes by simulating and graphing adversarial attacks paths against business process targets, configurations, and threats to assets. Security managers subsequently harden security infrastructure accordingly and therefore, systematically reduce overall IT security risks to the organization, periodically re-assessing risk and increasing threat intelligence (Hadar & Hassanzadeh, 2019). The tasks of performing remediation actions coincide with the need for security managers of government health organizations to understand the organizational security posture through security assessments and re-assessments. Subsequently, security managers prioritize, plan, and implement steps to maintain, strengthen, or expand that posture. Remediation action plans are provided as input into system authorization packages that certify and accredit systems and security controls.

Authorizing System and Security Controls

Authorization, on IT systems and security controls of U.S. government health organizations, is the output from authorizing officials that represents an approval to connect and operate systems and system controls within the live environment of the overall systems architecture of the organization (NISTJTF, 2018). Most security managers use authorization as the input to system or security control integration and organizational adoption. This process output is the product of systems that have demonstrated compliance by meeting specific security requirements regarding policy, components, documentation, and safeguards. Senior agency officials or authorized officials of the organization make risk-based decisions subject to the information system or control based on a thorough review of the information provided in an authorization package (NISTJTF, 2018). Authorization packages, varying between organizations, are a collection of documents that usually consist of plans, assessments, reports, and an executive summary that represent a common picture of the privacy and security posture of an organization about an information system or control (NISTJTF, 2018).

Alexander and Cummings (2016) highlighted that authorizing officials such as CIOs and CISOs face the challenges of adapting to the pace of technology and understanding the appropriate level of associated risk subject to authorizing systems and system security controls. Key attributes for authorizing officials have trended toward possessing a strong aptitude for communicating, influencing strategic direction, solutions-driven, understanding organizational mission, balancing priorities, and leveraging talent and resources (NISTJTF, 2018). Authorizing officials focus on these traits to understand the operational environment and security posture of the organization

for authorization package assessment and authorization of systems and system security controls. The U.S. Department of the Interior (2019) codified the assessment and authorization processes associated with systems and systems security into a method of evaluating how well a particular system design or implementation will meet mission objectives and security-based specifications. The processes have the three distinct phases of initiation (codification of security requirements), assessment (analysis of security controls in terms of correct implementation and effectiveness), and authorization (provides an official executive management decision of organizational acceptance) (U.S. Department of the Interior, 2019). System authorization is a supportive element of IT governance practices that are used to align IT infrastructure with business needs from the top-down approach of influencing policy, priorities, standards, vendor management, and project management (Gregory, 2017).

Risk responses are necessary for handling risk with the aspiration of influencing the achievement of the most optimal outcome for the organization (Boonjing & Pimchangthong, 2017). Typically, IT security managers, teams, and steering committees uncover and document relevant risks to systems and the organization (Fugini et al., 2016). Subsequently, security managers develop applicable risk responses approved and authorized by authorizing officials who are charged with making risk response decisions (NISTJTF, 2018). Documented risk responses are documented in security and privacy plans (Nikishova & Vitenburg, 2019). The more plausible organizational risk responses are mitigation (reducing risk possibility), transfer (passing on risk responsibilities to another entity), and acceptance (assuming minimal or residual risk) (Nan et al., 2016).

Moeini and Rivard (2019) proposed a model that focuses on the indirect influence and relationships of perceived risk exposure and IT project manager mediation and concludes that risk response attitudes are mostly influenced by risk-based decisions. IT security managers at government health organizations should be cognizant of the authorization processes involved with authorizing a system and associated security controls within the health organization (Abraham et al., 2019; Ahmed et al., 2019; Diehl et al., 2016; Frederick et al., 2017; Nikishova & Vitenburg, 2019). Security managers should also be fully aware of and document the requirements to develop thorough and complete authorization packages that detail the vulnerabilities, threats, relevant risks, and risk responses to the system and security controls (Emmerich et al., 2016; NISTJTF, 2018). This detail is relevant for the executive leadership or authorizing officials in hospitals and other government health organizations to make informed risk-based decisions on the security posture of the organization. Authorization processes set the stage for the systems and systems security to be monitored for effectiveness and efficiency (Adato, 2017; Ahmad et al., 2019; Awan et al., 2015; U.S. Department of the Interior, 2019).

Monitoring System and Security Controls

IT security professionals at government health organizations may find a significant benefit in monitoring the progress, effectiveness, and efficiency of organizational security investments (Thompson & Zandona, 2017). A good majority of government health organizations are subjected to constant and consistent pressure from threats (Jalali & Kaiser, 2018). Monitoring tools are implemented to enhance the monitoring capabilities of authorized systems and system controls implemented

throughout the organization (NIST, 2018). However, IT security managers must employ an integrated range of skills to understand the operational environment and recommend appropriate changes to the organizational infrastructure to properly prevent, detect respond to persistent threats (Abercrombie et al., 2017). Themes of the continuous and rapidly changing information technology environment were systemic throughout the literature. Monitoring IT systems and IT systems security platforms remains a critical element for the IT security manager to remain cognizant and address adaptive risks that influence required and approved changes in IT security infrastructure (Adato, 2017). Most cyber risk management methodologies address the continuously changing IT environment and subscribe to the practice of continuous monitoring of technology, human elements, and physical or environmental elements (NISTJTF, 2018).

Adato (2017) affirms that information systems and information system security monitoring are the consistent and continuous collection of metric data from physical and logical systems and advocates for the seamless collection of this data to influence actionable alerts and to develop and implement appropriate automated responses. Ahmad et al., (2019) states that information protection in organizations is influenced by the security assurance behavior of employees. The authors posited that the learned behavior of information security assurance is a trait of the human factor and can be enhanced by implementing information security monitoring as an encouraging factor that ranges beyond the security policies of the organization (Ahmad et al., 2019). Fugini et al. (2016) suggest the use of monitoring data through web-based tools to influence and facilitate dynamic risk management responses. The authors proposed an event-condition-action

(ECA) risk management methodology which focused on the elaboration of events and outputs through a unified dashboard of a web-based risk management system (RMS). The RMS provides information security managers with detailed information on potential organizational risks and suggested remediation strategies (Fugini et al., 2016). The web-based RMS supports the recognition of associated risks to systems and security controls, cooperation with the implemented access control system for prescribed rules and roles, and security-based intervention, modification, and risk-based knowledge management (Fugini et al., 2016).

IT security managers further enable and focus on monitoring IT systems and security controls by scheduling and conducting enduring security assessments, risk response updates, authorization updates, enduring security and privacy reporting, and system disposal procedures. NIST (2018) suggests implementing a continuous system-level monitoring strategy to support due diligence and adherence to authorizing official approved security specifications and strategy. Awan et al. (2015) defines the Risk Score method of continuously monitoring, assessing, and scoring risk, calculated using a correlation of traffic logs from security appliances such as the intrusion detection system/ intrusion prevention system (IDS/IPS) or firewall logs, defined by threat type quantities and conditionally based on threat intensity. The severity of threats is calculated by assigning an equidistant numerical value to each threat severity level representing low, medium, or high (Monken et al., 2017). Integrating a risk-scoring methodology quantifies continuous monitoring efforts to further support assessment reviews, understanding of

threat operational impacts, and probability, and enables risk-based decisions (NISTJTF, 2018).

Diehl et al. (2016) recommends the four-step process of developing a cyber risk management plan, establishing a cyber risk management team, assembling an external team of expert advisors, and collaborating with other industry professionals or consulting external industry institutions before developing a monitoring plan. Ellingson et al. (2017) insists the organization should invest in the human factor related to employee training and awareness as a breach prevention and insulation technique. Adato (2017) assert that cyber risk mitigation and system and control monitoring practices should also include detailing contractor expectations in service level agreements with third party security staff and thorough analysis and periodic assessment of their security capabilities. Most IT security managers schedule and conduct periodic assessments of IT systems and corresponding security controls (Adato, 2017; Ellingson et al., 2017). Assessment results are documented and shared with senior leadership within the organization for an ongoing common understanding of the security and privacy posture throughout the organization (Adato, 2017; Diehl et al., 2016; Ellingson et al., 2017; NISTJTF, 2018).

Transition and Summary

The purpose of this qualitative multiple case study was to explore the cybersecurity risk management strategies effectively used by IT security managers to safeguard PHI and PII from data breaches concerning U.S. government health organizations. The targeted population consisted of the IT security managers of 4 medium-sized government health institutions located in the mid-west region of the

United States. The findings of this study may contribute to social change by positively stimulating patient trust and confidence in healthcare systems and strengthening the commitments of healthcare professionals by emphasizing sincere patient privacy. The research in this study was guided by the conceptual framework of the PMT which investigates the outcomes of fear appeals on attitude change and examines influencing factors associated with appropriate courses of action to prevent the noxious occurrence. Rogers (1975) proposed that the three critical components of the PMT (a) the magnitude of adversity of a depicted event, (b) the event's probability of occurrence, and (c) the effectiveness of the protective response, appeal to the natural fear of unfavorable outcomes.

In Section 1, I focused on the foundation of my research and provided a background of the study and purpose as it pertains to the general and specific IT problem set targeted at IT security managers. Building on this basis, I detailed the nature of the study by referencing the methodology used and the research questions to shape the approach of data collection. Also included in Section 1, was an outline of the conceptual framework which informs this study. Other supporting elements of the foundation of this study are the operational definitions, the assumptions, limitations, and delimitations, and the significance of the study. Section 1 concluded with a detailed literature review that focuses on critical analysis and synthesis of scholarly works which builds on the problem, purpose, sources of research for this study.

In Section 2, I reiterate the research purpose and highlight the processes which organized and assisted in the research facilitation. In Section 3, I outline the (a)

presentation of the findings, (b) applications to professional practice, (c) implications for social change, (d) recommendations for action, (e) recommendation for further study, and (f) reflections. Lastly, I include a summary of the research findings and provide a study conclusion.

Section 2: The Project

Purpose Statement

The purpose of this qualitative multiple case study was to explore the cybersecurity risk management strategies effectively used by IT security managers to safeguard PHI and PII from data breaches concerning U.S. government health organizations. The targeted population consisted of the IT security managers of four medium-sized government health institutions located in the Midwest United States. The findings of this study may contribute to social change by positively stimulating patient trust and confidence in healthcare systems and strengthening the commitments of healthcare professionals to ensure patient privacy.

Role of the Researcher

The principal role of the researcher conducting a qualitative study is to ethically engage in the research processes of discovering, assembling, analyzing, and organizing research data and associated materials to reflect, share, communicate, and document the data (Hoadley et al., 2019). Böcher et al. (2016) noted that the role of the researcher is that of a scientist (providing scientific basis), integrator (translating scientific information into plausible arguments), and interpreter (scientific participation and contribution). The role of the researcher assumes that of a data collection catalyst when performing qualitative research (Leedy & Ormrod, 2016). Beail and Williams, (2014) posited that a researcher employing a qualitative methodology uses approaches such as generating research questions, conducting interviews, and data analysis.

I used a mixture of semistructured telephonic and video/virtual conference interviews in concert with historical organizational data analysis through an exploratory multicase design to conduct my study and facilitate participant dialog and collaboration. In a multicase design, semistructured interviews are conducted and subsequently analyzed within a descriptive qualitative construct intended to accurately convey relevant experiences of the participants (Berta et al., 2019). As a network engineer and information assurance manager in the U.S. Army for over 20 years, I have been familiar with government information system risk management processes using frameworks that were founded on the PMT concepts for system certification, accreditation, and security. As a benefit to my research, my experience helped provide the application context and enhanced the content of the research. I actively communicated with and gained approval from each participant in my targeted population.

Researchers are required to uphold ethical standards and adhere to the needs of the participants by ensuring they are in a safe environment, ensuring they are not subject to harm, and offering them the best terms for constructive correspondence after the interview (Konradsen et al., 2018). As an ethical consideration, the participants of this study were offered consent by email reply and active participation after they reviewed the associated consent form provided to express their willingness to participate in the research interviews. I also observed the conventions detailed within the Belmont Report of 1979 to preserve the ethical tenets of responsible human subject research throughout the study (see Adashi et al., 2018). I strived to achieve high-quality ethical research and gained the approval of the university research review (URR) and the Institutional Review

Board (IRB). My IRB approval number from Walden University was 08-13-20-0705871. The National Research Act of 1974 was passed to establish IRBs as the authority that provides oversight, ensuring the protection of human subjects (Buttell & Cannon, 2015).

Bero (2017) stated that bias is often conveyed in research and researchers should implement deliberate steps to reduce bias and make the sources of bias transparent. Many researchers have an understanding that bias manifests because of implicit or explicit assumptions stemming from any research method, but they often lack enough detail in the research procedures to implement an effective bias mitigation strategy (Connolly et al., 2019). Placing specific emphasis on case study research, Alpi and Evans (2019) stated that bias diminishes credibility and reliability regarding the procedures and processes used by the researcher. I mitigated bias by ensuring the experiences and observations of the research participants were the foundation of the study findings through the practice of member checking. Member checking is the process of sharing with the participant the researcher's interpretations of the data as a method of validating the observations and experiences of the participant (Bradshaw, 2002; Cole & Harper, 2012; Harvey, 2015).

Participants

Practicing a purposive sampling strategy, the participants I pursued comprised IT security managers in government health institutions located in the Midwest United States who had successfully adopted a risk management strategy. Sampling is the deliberate process of choosing contextual examples or participants who provide substantive data that is representative of a larger scale (Korstjens & Moser, 2018). Candidates for research were only considered eligible as participants if they had played a significant role in the

successful implementation and sustainment of a risk management strategy in a government health organization. Some examples of suboptimal recruitment of qualified research participant processes have historically been attributed to a lack of access to remote participants and arduous consent processes (Aziz et al., 2016). I solicited qualified research participants by an email that contained a letter requesting their participation and a letter of consent. Researchers of qualitative studies have used in-depth, unstructured interviews to collect data from participants as an exploratory measure (Abramson et al., 2019). In preparation for interviewing the participants, I effectively communicated and built a rapport with them to develop trust and foster an open and honest environment. During the interviews, I ensured both the open-ended questions and the sequence of the questions asked were identical for each participant interviewed. Arsel (2017) stated that although the interview process is a persistent and progressive way to seek new information to inform the overarching research question, researchers should also consider the context of the interview within the world of the participant. Diefenbach et al. (2019) stated that the researchers should have optimized recruitment approaches to yield the best recruitment and retention outcomes of research participants subject to the study. For this study, I obtained access to qualified participants from the publicly available information of each organization including participant contact information through the websites or directories of the organizations. Participants received an invitation letter, which introduced myself, my study, and its purpose along with an accompanying participant consent form.

Research Method and Design

This study used a qualitative methodology and followed a case study design. Given this architecture, I used a varied number of sources from which to collect and synthesize data into a well-rounded case analysis. The principle emphasis of the case study is to understand the *how* or the *why* surrounding a particular case or cases (Alpi & Evans, 2019). Because the study focused on the exploration of cybersecurity risk management strategies used by IT security managers in U.S. government health organizations, the qualitative research methodology was the most appropriate to facilitate an understanding of the phenomena in their natural setting and the associated human impacts through various mediums. Research participants have an individual voice through their personal experiences, and there is no data without the researcher's participation resulting in the researcher having insider involvement of the subject matter (Iguchi et al., 2018). I also used a case study design to facilitate the collection and synthesis of data within a case-based context and construction (Alpi & Evans, 2019).

Research Method

Qualitative methods tend to use behavior-based observations, document examination, and/or interview-based designs to annotate appropriate developments and behaviors surrounding the topic. The qualitative method is used to uncover knowledge, understandings, and meaning of phenomena through the experiences of people. A qualitative researcher employs independent methods in which the researcher does the data collection rather than relying on a mechanism, questionnaire, or device (Jobin & Turale, 2019). Some of the advantages of using qualitative methods are that researchers

usually immerse themselves within the natural surroundings of the research topic or subject to gain understanding through context. Research participants have an individual voice of their own through their personal experiences. There is no data without the researcher's involvement resulting in the subject matter (Iguchi et al., 2018). The justification of using a qualitative method is the need to study a topic within a native environment and to form an understanding or interpretation of a phenomenon's impact on people (Iguchi et al., 2018).

Quantitative methods are used to quantify developments, tendencies, and sentiments. A descriptive quantitative design is a nonexperimental design that describes relationships between variables using numbers, logic, and an objective stance (Siedlecki, 2020). The use of experimental design and quantitative methodology, typically support evidence-based decision making, building theory, policy discussions, and research. (Beretvas et al., 2014). Descriptive and experimental designs conducted for quantitative studies are not conducted in a natural setting (Carr, 1994). Therefore, the quantitative method was not appropriate for my study. An advantage of using a quantitative methodology is gaining unbiased research based on objectivity, control over redundant variables supported through the use of a lab environment, and theories that are tested through supported research (Iguchi et al., 2018). One of the disadvantages of quantitative research is that the experimentation conducted is not done in a natural setting (Carr, 1994). If the researcher misrepresents statistical data analysis in a controlled environment, proper interpretation could be lost (Drake & Jervis, 2014). A qualitative method was best for studying the topic of this research in a natural setting. Qualitative

research is used to understand human behavior, usually through the means of observing research participants and contributors and/or through various types of interviews (Iguchi et al., 2018).

Research Design

A qualitative research methodology using a multiple case study research design facilitates a comprehensive understanding of real-world problems through scientific investigation of phenomena, people, or a particular populace using natural and uncontrolled contexts (Korstjens & Moser, 2017). Qualifying considerations and primary dependencies about the case study qualitative design are the nature of the research, the desired scientific knowledge, and the research questions to be answered (Korstjens & Moser, 2017). Alpi and Evans (2019) state that the primary purpose of the case study is to understand the "*how*," the "*why*," and the "*what*" of a particular case without influencing the behavior of individuals involved and observing contextual conditions within unclear boundaries between context and phenomenon.

This study was best supported by using a multiple case study design-construct to more appropriately explore the cybersecurity risk management strategies effectively used by IT security managers to safeguard PHI and PII from data breaches concerning U.S. government health organizations. The multiple case study design enables the researcher to compare, understand similarities and differences, and replicate awareness of such findings across multiple case studies (Baxter & Jack, 2008). Therefore, using a multiple case study qualitative research design was contextually most suitable for this study to investigate, compare, and contrast the findings of multiple case studies surrounding the

practice of cybersecurity risk management in the mid-west region of the United States (see Stewart, 2012). Other qualitative research designs lacked the focus on case study comparisons, similarities, and variances to be appropriate for this study (see Polkinghorne, 2006). The narrative research design collects research data and formulates them into a story or stories for analysis (Casey, Corbally, & Proudfoot, 2016). This study did not communicate data collected into a narrative or reflective story (see Hickson, 2016). Therefore, the narrative research design was not appropriate for this study. Ethnographic designs focus on research that reports on experiences of a particular group differentiated by like characteristics such as origin or ethnicity (see Jong et al., 2018). This study did not focus on the experiences of segregated groups based on their similarities (see Kivunja & Kuyini, 2017; Walford, 2018). Therefore, an ethnographic design was not appropriate for this study. Phenomenology designs enables exploration of a phenomenon such as perceptions and meanings through general analysis (Arantzamendi et al. 2018). I did not seek to explore a phenomenon such as perceptions and meanings through general analysis (see Devadas, 2016). Therefore, phenomenology was not appropriate for this study. I employed the use of purposive sampling, member-checking, and triangulation to achieve data saturation. Researchers employ purposive sampling to recruit qualified participants knowledgeable of the research topic, therefore, the researcher may use small sample sizes to achieve data saturation (Patton, 2015). I used member checking to achieve data saturation, invoking the process of sharing with the participant the researcher's interpretations of the data as a method of validating the observations and experiences of the participant (see Harvey, 2015). Porcher et al. (2017)

states that achieving data saturation and ceasing the data collection process is the sole decision of the researcher based on experience and judgment. I used triangulation to support the integration and use of multiple data sources or avenues of data collection to mitigate bias, promote social change, positively influence data saturation, and add overall depth and reliability to the research (see Fusch et al., 2018).

Population and Sampling

The targeted population consisted of eight IT security managers of four medium-sized government health institutions located in the Midwest United States who have experience in cyber risk management process planning and implementation. I explored the strategies used by IT security managers concerning the implementation of a cyber risk management framework using data sourced from relevant participant interviews, observations, and organizational documentation. The selection criteria of interview participants stemmed from their breadth of experience with risk-based cybersecurity adoption and performing cyber-oriented risk management operations in a government health organization in the mid-west region of the United States. Individuals were not considered interview candidates who did not meet the criteria requisites of being an IT security manager (CIO, chief information security officer, IT security manager, IT risk manager, etc.) or lacked experience with or knowledge in IT, IT security, or IT risk management.

The type of sampling I used within qualitative research, was dependent on two primary factors: the research methodology and the topic studied (see Higginbottom, 2004). I used purposive sampling in my research to ensure my target population was

reached and to recruit only qualified participants with relevant background, experience, and knowledge to properly inform my study. Ames et al. (2019) states that too much data concerning qualitative evidence synthesis can destabilize the ability of the researcher to conduct a thorough analysis and purposive sampling is used to efficiently prioritize and manage data. I determined that suitable sample size to achieve the desired depth and multiplicity of perspectives for the study was eight IT security managers averaging two interviewees per organization from four participating health organizations. The number of participants was directly correlated to the number of participating government health organizations, providing either an initial or secondary perspective. Researchers employ purposive sampling to recruit qualified participants knowledgeable of the research topic, therefore, the researcher may use small sample sizes to achieve data saturation (Patton, 2015). Porcher et al. (2017) states that achieving data saturation and ceasing the data collection process is the sole decision of the researcher based on experience and judgment. I used triangulation to support the integration and use of multiple data sources or avenues of data collection to mitigate bias, promote social change, positively influence data saturation, and add overall depth and reliability to the research (Fusch et al., 2018).

Snowball sampling is a nonrandom method that allows the researcher to expand the sampling pool by receiving assistance from research participants in the participant recruitment process, therefore facilitating the prospect of gaining more participants that are considered relevant to the study (Emerson, 2015). Patton (2015) and Gelleri et al. (2017) suggest that recruiting participants using the snowball sampling method may pollute the results of the study as research informants may introduce a certain degree of

bias in the recruiting process. I sought to reduce bias to the lowest possible level and recruited qualified participants using unbiased recruiting techniques. Therefore, the snowball sampling method was not optimal for this study.

Random sampling is a technique that uses a selection method based on probability and makes it possible to provide every unit within the selection pool an equal and fair chance of inclusion (Lusinchi, 2017). Random sampling is more often used in quantitative studies than qualitative studies because of the coding and analysis indicative of random sampling (Dzhafarov, 2019; Emerson, 2015). I did not seek to randomly select participants for this study. Therefore, random sampling did not meet the requirements of this study.

Before the interviews were conducted, I accommodated each interviewee by allowing them to choose the virtual medium of the interview that was most convenient and comfortable for their situation. The premise behind this method, was to facilitate an environment that would positively influence the flow of receptive and candid dialog regarding interview participant question responses. Researchers, as an essential competency, should shape the interview environment to facilitate critical thinking, building trust, and focus on the process rather than the responses (Huang et al., 2019). I employed the use of purposive sampling, member-checking, and triangulation to achieve data saturation. Researchers employ purposive sampling to recruit qualified participants knowledgeable of the research topic, therefore, the researcher may use small sample sizes to achieve data saturation (Patton, 2015). I also used member checking to achieve data saturation, invoking the process of sharing with the participant the researcher's

interpretations of the data as a method of validating the observations and experiences of the participant (Harvey, 2015). Porcher et al. (2017) states that achieving data saturation and ceasing the data collection process is the sole decision of the researcher based on experience and judgment. I also used triangulation to support the integration and use of multiple data sources or avenues of data collection to mitigate bias, promote social change, positively influence data saturation, and add overall depth and reliability to the research (Fusch et al., 2018).

Ethical Research

Ethics is the foundation for conducting meaningful research and should be grounded on a practical and realistic evaluation of the potential harms or benefits to which the research participants are exposed to within the study (Herath & Rao, 2009). I ensured the study participants of the study confirmed their consent and overall willingness to contribute expressed through their review of the consent form and their subsequent active participation in the study. The consent form must be clear, detailed, and understandable to the potential research participant (Clark, 2019). In the consent form, I provided some background information on the study topic and discuss the participant procedures. The interviews conducted within a case study design regarding the relationship between the researcher and the research participants researchers may differ and in turn require flexibility and reflexivity (Creswell & Poth, 2018). I discussed the participant expectations and length of the interview and explain how the interview was documented and provided sample interview questions. I also discussed the voluntary nature of the study by detailing the risks and benefits as a participant. Lastly, I explained

that there will not be any compensation for their participation and I explained the right not to participate or discontinue participation from the research at any time. I provided each potential participant with an informed consent form.

I protected the participants and the organizations subject to this study by ensuring all data about this research was password protected for digital data and both physical and digital data and documents were stored in a locked filing cabinet at the residence of the researcher for no less than five years. Only the researcher of this study has access to the data. As the ethical duty, researchers are responsible for the protection of the rights of the participants, the protection of their confidentiality, and safeguarding information entrusted to the researcher (Sween-Cadieux & Turcotte-Trembley, 2018). To engage in research concerning human subjects, I have completed the collaborative institutional training initiative (CITI) Student Researchers Basic Course (Appendix A) and obtained the required certification. I received authorization to ethically solicit and interview participants from the Walden University IRB, approval number 08-13-20-0705871. After I received Walden University IRB approval, I sent a participant invitation letter, to each potential participant to introduce myself and to introduce the premise of the study. Once interest from the participants was established facilitated by the invitation letter, I sent the participant informed consent form to initiate the data collection process. Data collected about the research was stored on a password-protected solid-state drive and as the researcher, I locked physical information in a filing cabinet at my residence to which I only will have access. I will keep all data and information about the study for no less than 5 years after the study is completed. The participant names were substituted with the

letter “P” followed by a sequence number as a differentiating factor between participants and signifying the sequence a particular participant was interviewed. Other PII was not included in the study to ensure the confidentiality of each participant is always maintained.

Data Collection

Qualitative data collection is usually represented by verbalized participant accounts and observation filed notes, transcripts from interviews conducted, historical documents, journals, and literature from which thematic analysis is derived (Clark & Vealé, 2018). I used interviews as the primary method of data collection for this qualitative multiple case study. Interviews, such as face-to-face, telephonic, Skype, or email, are often used as data collection methods for thematic analysis considering qualitative research (Harcourt et al. 2018). The interviews conducted within a case study design regarding the relationship between the researcher and the research participants researchers may differ and require flexibility and reflexivity (Creswell & Poth, 2018). However, other forms of data collection such as observations, organizational documentation, notes, policies, procedures, and literature were also used in the data collection process. I ensured that I gained IRB approval and informed consent before beginning the data collection process.

Instruments

Qualitative studies emphasize the role of the researcher as the principal instrument in the data collection process to find, analyze, and interpret relevant themes or concepts (Nassaji, 2015). I collected research data by engaging each participant using 10

open-ended questions (Appendix B) in a semistructured interview framework. The data that I collected outlined the organizational implementation of risk management strategies focused on information protection. The interview questions also aided in gaining an understanding of the relevant experience and perceptions of the research participants relative to the strategies implemented. Data triangulation denotes the use of various types of data sources like observations, field notes, interviews, and organizational documentation to enrich reliability in the research findings (Mayer, 2015). Using the data collection protocol as a guide (Appendix C), I used data triangulation and ensured that the data collected was derived from various sources normally used in qualitative research to enhance data creditability and integrity. Farquhar et al. (2018) emphasized the use of data triangulation as a method of developing research trustworthiness within a study and recommends the use of interviews, company documents, and observations as relevant examples considering time and space. I mitigated bias by ensuring the experiences and observations of the research participants were the foundation of the study findings through the practice of member checking. Member checking is the process of sharing with the participant the researcher's interpretations of the data as a method of validating the observations and experiences of the participants (Bradshaw, 2002; Cole & Harper, 2012; Harvey, 2015).

Data Collection Technique

I scheduled 30 – 60-minute semi-structured interviews with each participant and ensured that the scheduled date, time, and virtual medium were mutually optimal. The semi-structured interview influences the process of establishing rapport with the

participant and facilitates a safe stage or environment for the participant and researcher to converse openly (Adni et al., 2012). Semi-structured interviews also offer an environment conducive allow the research participants to provide dynamic and detailed responses to the interview questions (Krauss & Peredaryenko, 2013). Dependent on the availability and geographic location of the prospective participant, interviews were conducted either telephonically or video/ virtual conferencing. Having alternative options available for the convenience of the participants concerning data collection techniques, increases the probability of interview invitation acceptance considering one method may appeal to a particular participant over others (Deakin & Wakefield, 2014; Rowley, 2002). As highlighted in the data collection protocol (Appendix C), I used multiple mediums to collect various types of data to create a holistic and well-rounded cyber-based risk management picture concerning health organizations. While considering the construct of data collection outlined in the data collection protocol (Appendix C), I used interviews and audio-recordings of the interviews, observations/ field notes, participants provided historical/ organizational documentation, and standard operating procedures (SOPs) as data collection methods. Denzin and Lincoln (2018) assert that considering the human interaction of the interview process and overall research, video and audio recordings provide a rich context for the study. Each interview included the same questions and sequencing highlighted in the data collection protocol (Appendix C). Researchers should take care to ensure neutrality and consistency during the semi-structured interview process to reduce bias, maintain control, and to influence knowledge-producing dialogue

by allowing the researcher to follow-up on aspects that are considered important for the study (Denzin & Lincoln, 2018).

After obtaining IRB approval, I conducted a pilot study consisting of one qualified interviewee as a pilot study participant from a health organization in the mid-western region of the United States. Safeguarding relevancy, the pilot study ensures study feasibility by gaging the research methods for practicality and succinctness from the perspective of the participant (Cole & Harper, 2012). I avoided data quality and integrity disruption and ensured the confidentiality of the participants by using alphanumeric code substitution to represent identifying information of the participants. Data organization techniques such as coding, the integration of field notes, and memos are used to support interpretive consistency and reflexivity (Humble & Radina, 2019). Following the pilot study, I followed up with each participant to verify the practicality and succinctness of the research questions and data collection methods used. Once the pilot study was complete, I then contacted potential study participants using the participant invitation letter and subsequently sent the informed consent form. Following positive feedback from the participant invitation letter and participant review of the informed consent form, I moved forward with the data collection process and scheduled either video/ virtual conferencing or telephonic interviews with the remaining qualified participants. At the start of each interview and after introducing myself, I gained verbal consent, outlining the purpose of the study and highlighting key elements of the pariticpant-reviewed informed consent form, and specifically emphasized the intention to audio-record and transcribe the interview. The interviews continued with the interview questions after verbal consent

was provided. After the interview and the associated transcription was complete, I forwarded a copy of the summarized interpretation of the data collected to each participant for verification of accuracy prior to performing data analysis. I mitigated bias by ensuring the experiences and observations of the research participants were the foundation of the study findings through the practice of member checking. Member checking is the process of sharing with the participant the researcher's interpretations of the data as a method of validating the observations and experiences of the participant (Harvey, 2015).

Data Organization Techniques

Researchers face the challenges of anonymizing research material to protect the confidentiality of the participants without inadvertently undermining the integrity and quantity of the data (Surmiak, 2018). Data organization techniques such as coding, the integration of field notes, and memos are used to support interpretive consistency and reflexivity (Humble & Radina, 2019). I transcribed the audio recorded interviews and safeguarded the documents on a password protected solid-state drive. Sween-Cadieux and Turcotte-Trembley (2018) state that researchers must be understanding of the challenges of organizing large amounts of data, maintain consistency in coding, and use strategies that enable them to continually respect the privacy of participants while handling potentially sensitive data. I used the NVivo, release 1.3, and Dedoose software platforms to assist with coding, data protection, and data organization. All data about this study was either password-protected for digital data or stored in a locked filing cabinet at the residence of the researcher for at least five years for physical documents.

Data Analysis

For this qualitative multiple case study, the primary methods of data collection were semi-structured interviews, field notes, and relevant and supporting documents such as SOPs, policies, and other documentation from participants of participating organizations. Organizational documents are primarily used in research to confirm the findings of other sources (Alpi & Evans, 2019). Triangulation supports the integration and use of multiple data sources or avenues of data collection to mitigate bias, promote social change, positively influence data saturation, and add overall depth and reliability to the research (Fusch et al., 2018). There are four fundamental forms of data triangulation: methodological triangulation (using several methods for one problem), investigator triangulation (using several researchers), theory triangulation (using different interpretation viewpoints), and data triangulation (using different data sources) (Patton, 2015). I integrated the data triangulation methodology as a data analysis technique to compare and contrast data elements and to assist with providing depth and reliability to the study.

During the scheduled interviews, I asked each participant for releasable and supporting organizational documentation such as SOPs, policies, or any other supporting documents appropriate for the interview not publicly accessible to further substantiate participant accounts. I also reviewed all supporting documentation and ensured to capture relevant information to the study using field notes and I audio recorded each interview, (with participant consent), to support the transcription process. Post-interview, I shared the summarized interpretation of participant accounts and the generated coded themes

with the participants to provide them the opportunity to verify the accuracy of their responses and their intent. Bonfils, Firmin, Luther, Minor, and Salyers (2017) endorses the use of software programs to assist researchers with quickly labeling text, assigning relevant codes throughout transcripts, and providing visual context to enable research analysis. I used the NVivo software and the Dedoose software platforms as tools to assist with data organization and coding the relevant qualitative themes while performing thematic analysis. Thematic analysis is a method to ensure identification and theme reporting within the construct of data analysis (Patton, 2015). Upon completion of the member checking process and thematic analysis, I performed data analysis and synthesized the generated themes into a coherent final interpretation of the cases relevant to the conceptual framework of my study. Harvey (2015) mentions that the combination of transcription (documenting verbal accounts), member checking (participant validation), and analysis enhances the validity, accuracy, and overall credibility of the study.

The conceptual framework used to inform this study was the PMT and exhibits relevance to this study by exploring the inherent and fundamental concepts of risk management as they relate to safeguarding PHI and PII to avoid or prevent the noxious events of data breaches (Rogers, 1975). Serving as the supporting methodology between the research conducted, the findings generated, and the reinforcing literature, the conceptual framework is the foundational element within the study (Snelgrove & Vaismoradi, 2019). The themes that were developed and organized into relevant categories from data analysis will validate the PMT contribution to influence the privacy

and protection of health-oriented data and secure health information management today (Herath & Rao, 2009).

Reliability and Validity

Strategies to develop and maintain the reliability and validity of the data within this study will be provisioned for and implemented to mitigate associated threats. Cypress (2017) asserts that reliability and validity are important components of qualitative research and exemplify a particular degree of rigor on behave of the researcher. In quantitative research, reliability represents the consistency of the research processes and the results and is the product of refutational analysis, comprehensive data, and data comparison (Leung, 2015). Validity represents the appropriateness of the tools used, the processes, and the data subject to developing a qualitative study (Leung, 2015). To mitigate associated risk concerning the reliability and validity of the research, I used several methods that compared and contrasted the comprehensive data gained and I integrated techniques and tools to support the appropriateness of the instruments, processes, and data used to research this study.

Researchers who work within the qualitative research paradigm should seek to establish the trustworthiness of their research defined as dependability, creditability, transferability, and confirmability (Amankwaa, 2016; FitzPatrick, 2019; Guba & Lincoln, 1985). Amankwaa (2016) elaborates that researchers should create protocols used as a framework for establishing credibility (truth confidence in findings), transferability (contextual applicability of findings), dependability (consistent and repeatable findings), and confirmability (extend findings are shaped by respondents). I ensured the research

conducted for this study developed and maintained value by enveloping practices and procedures to systematically integrate the trustworthiness pillars of dependability, creditability, transferability, and confirmability.

Reliability

As a researcher, I sought research approaches and practices that continuously and consistently assisted in obtaining, improving, and maintaining reliable data and represent true assumptions and viewpoints of the participants subject to this study. In qualitative data collection, textual and audio sources are thought to have a solitary meaning and are interpreted accordingly (Ergun, 2017). I reviewed and subsequently interpreted all textual and audio data collection for completeness and context. Researchers of qualitative studies use the trustworthiness pillar of qualitative dependability as the essence of reliability which often is the product of data comparison and the use of comprehensive data (Leung, 2015).

Dependability

Threats to dependability may be mitigated through the practice of verifying the accuracy of sources using constant comparison and triangulation (Leung, 2015). Dependability is a supporting element of research reliability and assists with the quality and confidence of the synthesized findings (Abler, Khoza, MacPhail, & Ranganathan, 2016; Aromataris, Lockwood, Munn, Pearson, & Porritt, 2014). Focusing on research dependability, I used the study protocol for the organization (Appendix C) and the NVivo and Dedoose software platforms for coding and case study database management.

Various coders are employed for facilitating coding consistency and thematic analysis and improve the reliability of the study (Ergun, 2017).

Validity

FitzPatrick (2019) states that validity is the comprehension and measurement of trustworthiness that depends on the research context, purpose, and ability to address threats to soundness and rationality of the research results over data. Using member checking, I reduced researcher bias and confirmed the accuracy of participant accounts, and enhanced the trustworthiness of the study. Researchers as data collection instruments use member checking as a method of participant validation to confirm the trustworthiness of qualitative results (Birt, Campbell, Cavers, Scott, & Walter, 2016). As the primary requisite to quality research findings, validity is the product of the accuracy of the research from the perspective of the researcher, participants, and research reviewers (Lub, 2015).

Credibility

Credibility also denotes trustworthiness as rigor is established in qualitative research by which there is a myriad of strategies to strengthen internal validity and believability of the findings (DeCino & Waalkes, 2019). Cope (2014) defined credibility as the truth represented by genuine participant views that are accurately interpreted by the researcher. Data triangulation implies the use of various types of data sources like observations, field notes, interviews, and organizational documentation to enrich reliability in the research findings (Mayer, 2015). I used data triangulation and ensured that the data collected was derived from various sources normally used in qualitative

research to enhance data creditability and integrity. Farquhar et al. (2018) emphasizes the use of data triangulation as a method of developing research trustworthiness within a study and recommends the use of interviews, company documents, and observations as relevant examples considering time and space.

Transferability

Transferability signifies the portability of the study findings and speaks toward their application to various settings or groups outside of the study (Cope, 2014; Ferrando, et al., 2019; Guba & Lincoln, 1985). I provided an appropriate variety of supporting information for the readers of this study to assess the capabilities and transferability. I integrated transferability throughout this study and use the data collection protocol as the catalyst to integrate transferability in the interview process to ensure such considerations are deliberated. The data collection protocol was the guideline that assisted the interview process by ensuring that pertinent information is conveyed to the interviewee such as reaffirming the primary objective of the interview, addressing concerns related to confidentiality, integrity, and availability of data during and post-interview (Patton, 2015). Transferability in the context of qualitative ensures participants subject to the study are provided the opportunity to respond to the same questions, ensuring comprehensive findings of the qualitative research subject matter (Patton, 2015). Using transferability throughout the qualitative research process will also provide other researchers with the opportunity to build correlations and expand from my research.

Confirmability

Confirmability is the process and practice of reducing researcher bias and ensure reflexivity (Cope, 2014; Fusch et al., 2018; Guba & Lincoln, 1985). As the research instrument, I positively influenced confirmability by maintaining a reflective research log or journal to accurately record participant thoughts, emotional content, and participant feelings. I also conducted member checking to ensure the sentiment of the participants was accurately interpreted. Member checking is the process of sharing with the participant the researcher's interpretations of the data as a method of validating the observations and experiences of the participant (Bradshaw, 2002; Cole & Harper, 2012; Harvey, 2015).

Porcher et al. (2017) states that achieving data saturation and ceasing the data collection process is the sole decision of the researcher based on experience and judgment. A key aspect to realizing data saturation in qualitative research is understanding and assessing the natural culmination of the research signified by the inclusion of all necessary data to adequately answer the research questions (Babbage et al., 2018). Researchers employing purposive sampling to recruit qualified participants for the study can use small sample sizes to achieve data saturation (Bernard, 2013). While researching this study, I ensured that I employed the tools of purposive sampling, triangulation, and detailed participant interviews aimed at answering the research question.

Transition and Summary

The purpose of this qualitative multiple case study was to explore the cybersecurity risk management strategies effectively used by IT security managers to safeguard PHI and PII from data breaches concerning U.S. government health organizations. The targeted population consisted of the IT security managers of 4 medium-sized government health institutions located in the mid-west region of the United States. The findings of this study may contribute to social change by positively stimulating patient trust and confidence in healthcare systems and strengthening the commitments of healthcare professionals by emphasizing sincere patient privacy. The research in this study is guided by the conceptual framework of the PMT from which the basis is the observed correlation between perceived magnitude and potential of noxious events and protection motivation to relatively respond to those events. In Section 2, I reiterated the research purpose and highlighted the processes which will organize and assist in the proposed research facilitation. In Section 3, I outlined the (a) presentation of the findings, (b) applications to professional practice, (c) implications for social change, (d) recommendations for action, (e) recommendation for further study, and (f) reflections. Lastly, I included a summary of the research findings and provide a study conclusion.

Section 3: Application for Professional Practice and Implications for Social Change

Introduction

The purpose of this qualitative multiple case study was to explore the cybersecurity risk management strategies effectively used by IT security managers to safeguard PHI and PII from data breaches concerning U.S. government health organizations. The participants of this study comprised eight IT security managers of four medium-sized government health institutions located in the Midwest United States. All participants in this study met the participant qualification standards of having experience in a role that influenced the successful implementation and sustainment of a risk management strategy in a government health organization. The data in this qualitative multiple case study was derived from an amalgamation of semistructured interviews, field notes, and relevant and supporting documents such as SOPs, policies, and other sources from each participating organization. The four overarching themes that derived from the research and supported effective cybersecurity through risk management were: (a) structured, systematic, and timely cyber risk management; (b) continuous and consistent assessment of the risk environment; (c) system and controls development, implementation, and monitoring; and (d) strategy coordination through centralized interagency and interdepartmental risk management. Participants collectively viewed cybersecurity through risk-based strategies implementation as the catalyst to ensure data breach reduction. In Section 3 I present the findings, their application to professional practice, and implications for social change. Also included in Section 3 are the recommendations for action and recommendations for further research pertaining to

achieving cybersecurity using risk management strategies of U.S. government health organizations. Concluding this study are my reflections about the study process and a final statement.

Presentation of the Findings

The primary research question for this qualitative multiple-case study was:

RQ: What are some security strategies used by IT security managers to effectively safeguard PHI and PII from data breaches concerning U.S. government health organizations?

The primary methods of data collection were semistructured interviews, field notes, and relevant and supporting documents such as SOPs, policies, and other sources from participants of participating organizations. The findings comprised the experiences of the IT security managers regarding protecting the sensitive information of U.S. government health organizations from data breaches. I maintained the confidentiality of the participants by substituting their PII with nonidentifying alphanumeric naming conventions for all eight participants expressed as P1 through P8. The interviews were conducted using multiple virtual means at the preference of each participant. I recorded, transcribed, and appropriately coded the responses of each participant to the interview questions (Appendix B). I used the NVivo 1.3 software to assist with coding, data protection, and data organization, and I also used the Dedoose software as a cross-reference platform to discern and analyze major themes associated with the data received from the participants and assist with coding, data protection, data organization, and open-source documents. I also used methodological triangulation to compare and contrast data

received from the participants and open-source data elements and to assist with bias mitigation and providing depth and reliability to the study.

Table 1

Summary of Primary Themes

Primary themes	% of participants referencing the theme	# of references by the participant and organizational documentation
Structured, systematic, and timely cyber risk management	100%	8 participants and 4 organizational documents
Continuous and consistent assessment of the cyber-risk environment	87%	7 participants and 8 organizational documents
System and controls development, implementation, and monitoring	100%	8 participants and 11 organizational documents
Strategy development and coordination through interagency and interdepartmental risk management	75%	6 participants and 4 organizational documents

Theme 1: Structured, Systematic, and Timely Cyber Risk Management

Most interviewed participants mentioned a general need for a systematic, structured, and timely approach to risk management with greater emphasis on implications of cybersecurity. P1, P3, P4, and P7 emphasized the importance of implementing cyber risk strategies structured around conformance with governmental and organizational policies, standards, and regulations. All four health organizations used the NIST RMF, NIST Cybersecurity Framework, and NIST federal information processing standards (FIPS) as the foundation of cybersecurity risk management with their enterprise security strategy. Partial legitimacy of the security assessment program in the healthcare industry is dependent upon its adherence to general organizational governance under laws, regulations, and organizational policies and objectives (Chen et al., 2019).

P2, P4, P7, and P8 echoed the sentiment of governance structure conformance serving as contributions to successful cyber risk strategies and expanded by also emphasizing the importance of well-defined roles and responsibilities within the health organization regarding successful risk management strategy. Notably, P4 drew specific attention to the roles of the CIO and CISO stating, “Those affected by information systems would be best served through a separation of the CIO and CISO roles as two distinct equal pillars.” This proposal advocates for a strategically-oriented and equal voice at the executive level concerning security embedded in IT architectural design and relevant organizational activities. In accord with this, NISTJTF (2018) aligns the assignment of key stakeholders and appropriate roles and responsibilities with proper

risk-based preparation and understanding of the organizational strategy for approaching threats and of cyber risk tolerance levels within the risk environment. Two of four organizations stressed the recruitment and retention of the cybersecurity workforce to emplace talent where warranted.

P2, P3, and P8 expressed focusing on systematically evaluating and responding to cyber risk to effectively safeguard data processed through organizational information systems. P3 elaborated further on systematic processes regarding cybersecurity and risk management stating that "systematic risk management is the cornerstone of securing the information technology environment and is critical to delivering actionable cybersecurity strategy." Supportive of this concept, Boonjing and Pimchangthong (2017), Fugini et al. (2016), Gan et al. (2020), and Keenan et al. (2016) proposed that preparing a government health organization to adopt effective cyber risk management processes similar to any other organization and industry requires an assessment of relevant risks as they pertain to a given system or system implementation and the likelihood of realized threat impacts. The security of systems in a government health organization may be dependent on a thorough risk assessment, the analysis of the associated outcomes, and the risk relevance to the organization and its stakeholders (Ammenwerth & Leber, 2017; Belaissaoui & Elkhannoubi, 2015; Jalali & Kaiser, 2018; Retnowardhani & Yoseviano, 2018).

P2, P7, and P8 accentuated that timely and dynamic approaches to implementing elements of cyber risk strategy influence effective cybersecurity. P2 reinforced the concept of a timely approach by stating, "Defending the cyberspace ecosystem is influenced by enhanced timely detection of cyber threats, intrusion detection, and

situational awareness." Alshawish et al. (2019) suggested using an easy to understand, scalable, and a TTC comparative security metrics highlighting remedial cybersecurity development derived from the potential time an adversary needs to exploit a system vulnerability. Building on security remedial action development, Hadar and Hassanzadeh (2019) stated that planning and prioritizing remedial security actions are a product of relevant levels of risk and can be performed under agile security processes by simulating and graphing adversarial attack paths against business process targets and configurations and threats to assets.

According to Rogers (1975), the probability of realizing a noxious event comes from the fear of pertinent, plausible, and previously experienced risk. The PMT focuses on risk responses that, guided by the magnitude and probability of the event and the efficacy of risk-based controls, developed from systematic, structured, and timely approaches to cyber risk. Rogers (1975) proposed that organizational structure and defined roles and responsibilities effectively promote proactive and reactive change by invoking the cognitive mediating processes outlined in the PMT to systematically evaluate the noxiousness, probability, and severity of risk and the effectiveness of a timely risk response. Therefore, the theme centers on IT security managers implementing risk-based organizational structure, systematic processes, and calculated approaches to cyber risk management, supporting implementation of effective controls structured to limit probability and magnitude of data security breaches based on relative protection motivation.

Theme 2: Continuous and Consistent Assessment of the Cyber Risk Environment

Some participants in this study and all of the risk-oriented organizational documentation such as strategies, frameworks, and standards of the participating institutions make significant mention of the value behind conducting a continuous and consistent assessment of the cyber-risk environment. All of the participants, in some form or another, recognized that security threats to and weaknesses of the health organization are identified through the systematic, periodic, and complex processes of risk assessments, subsequently provisioning for the adoption of the appropriate solutions to respond to risks. As a generalized consensus amongst the participants and the organizational documentation, risk-based assessments are performed to both understand the present and organizationally relevant cyber threat environment and to understand the efficacy of associated controls.

Specific to the reference of continuous and consistent assessment of the cyber-risk environment in terms of processes, P5 mentioned, “Systems are categorized following FIPS, assigned security controls which are routinely tested, evaluated for an authorization to connect [ATO] by an authorizing official, and periodically and randomly scanned and assessed for anomalous behaviors or activities outside of the scope of the ATO.” P3 elaborated further regarding continuous and consistent assessment by stating, “There are many good policies, procedures, tools, and personnel available, but if they are not implemented properly, and periodically independently validated to ensure proper implementation, they won’t be effective.” As a reference to the perspective of the IT security manager concerning the value of assessments, P4 stated, “From my perspective,

the most important aspect for leadership is having a periodic independent assessment of their security program – relying on internal self-assessments that 'all is good' is woefully insufficient."

Several cyber risk-oriented organizational documents of the participating government health institutions focused on comprehensive risk analysis which demands accurate and thorough assessment of the potential risks and vulnerabilities to all three elements of the CIA triad: confidentiality, integrity, and availability of PHI. Moreover, the documentation I reviewed outlined that assessments are valued sources of information that contribute to the identification of technical vulnerabilities in information systems and processes. Agreeably, NIST (2010) proposed that assessment plans need to be provisioned, approved, and updated based on security and privacy strategies and business objectives, control assessments, and ensure reports are maximized through automation. Rashidi and Shakibazad (2020) advocated for using risk identification and risk assessment methods within the construct of the risk management processes to adequately analyze the risk sensitivity of organizational assets to determine the potential risks. According to Rogers (1975), the PMT is driven by the phobia-based perceptions of realized risk preemptively assessed by the organization. The information provided by the participants and the organizational documentation which were aligned with this concept evidenced that the perceptions of IT security managers are, at a high-level, contributive of the continuous and consistent assessment requirements of the cyber-risk environment. The fear of realized risk drives the action of maintaining data and knowledge derived from systems, people, and processes through assessments to appropriately identify and

respond to risk to prevent breaches in information security. Moreover, the frequency of the assessments outlined in organizational policies and procedures was directly related to the desire for up-to-date accurately associated organizational cybersecurity risks to systematically influence the dynamic understanding of the cyber environment.

Theme 3: System and Controls Development, Implementation, and Monitoring

Each study participant specifically referenced the development of cybersecurity systems, processes, and organizational climate in terms of controls, to include the implementation of those mentioned controls and the subsequent continuous monitoring that operates as and in concert with routine organizational operations. P1, P4, P5, and P6 have independently made a stance toward cybersecurity or controls-based architecture, highlighting the processes of systems and services controls selection and integration into the greater information technology architecture. P1 specifically emphasized the development of controls by directly stating, “Threat protection starts with development.” Additionally, P5 stated, “We determine the risk of systems and ensure the proper controls are being applied in the development and the production environment.” The relevance of the PMT, complementary theories, frameworks, and regulatory guidelines and standards for present-day application as they assist IT security managers of U.S. government health organizations in a data breach is solidified through the development of a risk-based context and setting the priorities for cybersecurity risk management and promote the perpetuation of privacy and security (Aljohani et al., 2018; Kim et al., 2018; Johnson & Kwon, 2015; Rezaeibagha et al., 2015; Small & Wainwright, 2018).

Implementations of physical security controls are designed to protect data by placing security measures at the point of presence to both physically prevent and possibly deter unauthorized access to sensitive data management mediums (Abercrombie et al., 2017; Cohen et al., 2015; Hillebrand et al., 2016; Liu et al., 2016). P4 focused on IT system scanning, specifically emphasizing discovery, configuration, and vulnerability, stating, “To protect your IT systems, you must know what is on them or connected to them, and that they are securely configured, especially if IT staff are given the relative autonomy to connect devices at will (vs. in a more controlled environment, where a device must go through an independent review process before it can be connected).” P6 elaborated further by stating that, “IT systems should be frequently scanned for new devices and all devices should be frequently checked for proper configuration and the remediation of all known and unacceptable vulnerabilities.” Both P4 and P6 credited that performing the aforementioned activities in near real-time provides leadership with the most accurate and complete view of their IT systems. Rotella (2018) concluded that the security control baselines of the organization aid IT security managers by providing a point of reference for vulnerability management within the organization, and without this reference, security engineers are challenged in providing effective security measures.

Most participants to exemplify specific considerations related to control categories, outlined technologies, services, and processes that contributed to the over security and access control architecture that were based on mitigating organizational risks. P2 highlighted efforts to mitigate risks through the use of multifactor authentication by stating, “two-factor authentication, such as through the use of a card and PIN as is

often used with Automated Teller Machines (ATMs), ensures only authorized personnel can access your IT systems. P4 expanded on the implementation of multifactor authentication by stating, “Multifactor authentication for all levels of access is crucial in the current environment; it helps ensure account integrity and has the added benefit of ease of use for end-users.” Other implementations of cyber and information security controls highlighted by several participants were the integration of antivirus, firewalls, intrusion detection/ prevention systems, encryption, and the practice of network segmentation. P3 outlined specific risks that are usually mitigated using antivirus, firewalls, and intrusion detection/prevention in terms of employing packages of endpoint security, saying “IT system users will inadvertently or even intentionally perform some actions that may be detrimental to IT systems, such as opening e-mail attachments from untrusted sources or visiting malicious web sites.” P7 focused on the implementation and continued employment of encryption throughout the security architecture stating, “Ensuring all devices that can be encrypted are encrypted and using FIPS-approved cryptographic modules, protects the information on those devices from unauthorized access, theft, or inadvertent release (such as when selling, donating, or discarding outdated equipment).” Advocating for network segmentation, P8 emphasized that multiple networks and subnetworks may be employed to more easily restrict access to data on those networks based on a need to know and to also limit adversarial lateral movement in case of compromise. An assessment of technical security controls usually investigates technologies such as encryption, authentication, an automated process of

access controls, certificates, and file integrity (Cohen et al., 2015; Hillebrand et al., 2016; Jurn et al., 2018).

The majority of the study participants also highlighted the practice of monitoring security controls about their performance in mitigating cybersecurity risks. Most security managers in government health organizations will assess the effectiveness of technical security controls through automated processes and various other means (Abraham et al., 2019; Ahmed et al., 2019; Diehl et al., 2016; Frederick et al., 2017; Jalali & Kaiser, 2018; Mariani et al., 2015). IT security managers should document planned control implementation and the monitoring strategy for the control systems (Fuchs et al., 2016; Kulkarni, 2019; NISTJTF, 2018). P6 specifically discussed organizational procedures regarding monitoring cybersecurity controls, outlining, “An Information System Security Officer is assigned to each system, assisting Information System Owners to ensure staff is periodically monitoring systems, creating, and resolving plans of action and milestones where applicable.” All organizational information security policies reflected a sustaining requirement to consistently and continually monitor information security controls. Managed as a cybersecurity objective, language used throughout various organizational documentation illustrated and emphasized the management of risk through continuous monitoring, diagnostics, detection, and accelerated adoption of tactics, techniques, and procedures from lessons learned and mitigation plans. The three components are described as (a) the magnitude of adversity of a depicted event; (b) the event's probability of occurrence; and (c) the effectiveness of a protective response (Rogers, 1975). Relevant to the conceptual framework and IT practice, IT security managers benefit from

accurately assessing the magnitude of adversity regarding organizational security threats and the subsequent assignment of protective and comparable risk responses through the development of security controls. Rogers (1975), submitted that the probability of adverse events can be evaluated through active monitoring of security controls.

Theme 4: Strategy Development and Coordination Through Interagency and Interdepartmental Risk Management

Strategy development and coordination through interagency and interdepartmental risk management was not the most prominent theme amongst the interviewees in comparison to the other themes. However, the combination of emphasis between both the participants and the organizational documentation reflected the need for IT security managers to understand and employ centralized and coordinated processes throughout each organizational echelon. This practice emphasizes major contributions to coordinating multidisciplinary cybersecurity and risk management operations. Kuzmenko et al. (2020) emphasized that the higher the level of threat the more the need for various internal and external organizational echelons and entities to combine and coordinate efforts to create holistic risk management and cybersecurity system and governing framework. Such a predominant entity would serve as a singular information infrastructure and an overarching authority to protect against cyberthreats, cyberterrorism, and cyberespionage. Notably, P2 addressed organizational concepts of centralized and joint healthcare-specific cybersecurity and risk management by stating that it “reduces the reliance on hard copy data and the potential for human error in entry

of data." Moreover, P8 mentioned, "information is jointly shared with the contractor, the Department of Defense, and VA for incorporation into their security processes."

The data collected which pertained to this theme focused on maintaining a comprehensive, centralized, cooperative, and coordinated cyber risk management strategy. Several documentations from organizations subject to this study suggested that the is a critical need to coordinate efforts across echelons to ensure mutual and balanced cyber risk management achieved both through centralization and overarching management. Executive Order 13636 (2013) is the presidential policy of the Obama administration, guiding cybersecurity initiatives of government organizations. Specifically, these initiatives were directed toward, as the title suggests, improving the cybersecurity of critical infrastructure. This policy, more relevant to this study, also provides cybersecurity infrastructure guidance for government health organizations. Emphasizing cybersecurity information sharing, the policy states that influencing greater volumes, timeliness, and quality of shared cyber threat information is a product of the coordination between the U.S. Attorney General, the Director of National Intelligence, the Secretary of Homeland Security, and the U.S. private sector. Relevant to U.S. government health organizations, this interagency and interdepartmental risk management coordination within the U.S. government, assists in the facilitation of risk reduction planning influenced by a shared understanding of the cyber threat environment across organizational entities and echelons.

P5 described the prospect of successful cyber risk management largely contributive to timely and deliberate cyber risk information exchanges and threat analysis

between the various health organizations in the U.S. government. P7 highlighted that "cyber defenders in healthcare can exponentially increase advantages regarding cybersecurity by sharing cyber risk and cyber threat information with each other." Bohme and Laube (2017) stated that cyber risk information sharing is a trivial and inexpensive method to assist defenders to build mutual trust and expected cyber risk reductions.

Organizational documentation comprising of enterprise strategy and associated policies thematically focus on the need to view cyber risk management under the structured approach of creating risk-oriented profiles. The risk profiles are developed and linked primarily through communication, collaboration, and cooperation between entities that support information technology divisions; quality, performance, and risk programs and offices; and IT modernization programs that contribute to enterprise risk management activities considering each government health institution. The risk profiles inherently provide leaders a common site picture of risks that affect various information technology divisions within U.S. government health organizations and identify synergies for risk response. The conglomerate of organizational documentation regarding cooperative and coordinative information sharing amongst government entities focus on four fundamental risk areas: the effectiveness of the privacy program, the efficacy of electronic records management, information technology modernization, and the human element considering processes, procedures, and training. The Cybersecurity Information Sharing Act (CISA) of 2015 provides a foundational concept of information-sharing regarding government entities leveraging interdepartmental, interagency, and private sector cybersecurity information sharing (Cybersecurity Information Sharing Act of

2015). According to Rogers (1975), the PMT focuses on identification and avoidance or prevention of noxious events which cause uncertainty in the security posture of the organization. Kwon, Lee, and Yang (2020) concluded that introducing CISA plays a vital role in reducing uncertainty and ultimately decreasing cyber risk on a large scale. As a relevant theme to information technology practice, strategy development and coordination through interagency and interdepartmental risk management help IT, security managers, in U.S. government health institutions to identify cyber threats and associated cyber risks as a means to reduce the uncertainty developed from noxious events and provide a conduit to implement comparable controls.

Application to Professional Practice

In light of the increasing dependence on information technology, cybercrime has taken advantage of pandemic also increased and is forecasted to reach global scale costs of over $6 trillion by 2021 (Chakravarthy et al., 2020). According to Frederick et al. (2017), U.S. government health organizations should be particularly concerned as the foremost cause for cybersecurity breaches regarding PII and PHI are realized risks from cyberattacks. Lo et al. (2018) states that there has been at least $7 billion worth of annual losses related to breaches in information security within the healthcare industry. The healthcare industry has fallen prey to cybercrime and data security breaches even more than the financial industry since 2016 and more likely will see exponential increases of cybercrime opportunities from the onset of global pandemics such as COVID-19 (Chakravarthy et al., 2020).

Relevant to the application to professional practice, the aforementioned themes of this study illustrate industry trends that reflect a specific emphasis on the application of risk management concepts as they relate to disabling events leading to data security breaches. Operating as the foundation of these concepts are the fundamental elements of the PMT: the magnitude of adversity of an event, probability of occurrence regarding the event, and the effectiveness of a protective response which also works collaboratively as functional considerations pertinent to cybersecurity. IT security manager participants of this study within participating U.S. government health organizations have seen successful or improved cybersecurity measures through the implementation of structured, systematic, and timely cyber risk management practices and risk responses. Ellingson et al. (2017), Frederick et al. (2017), and NISTJTF (2018) focus on the premise of IT security professionals following best practice practical design principles that adhere to more comprehensive protection and control of systems. The consensus among the participants and organizational documentation regarding this theme have forecasted cybersecurity success through the implementation of comprehensive organizational cyber risk strategy; conformance of governmental and organizational governance; and well-defined roles and responsibilities conducive to risk triage.

Participant interviews and methodical review of publicly available organizational strategy, policies, and other supportive documentation have inferred that successful cybersecurity strategies of U.S. government health organizations call for the integration of continuous and consistent assessment of the cyber-risk environment. The security of systems within a government health organization may be dependent upon a thorough risk

assessment, the analysis of the associated outcomes, and the risk relevance to the organization and its stakeholders (Ammenwerth & Leber, 2017; Belaissaoui & Elkhannoubi, 2015; Jalali & Kaiser, 2018; Retnowardhani & Yoseviano, 2018). The data collected related to the theme of continuous and consistent assessment of the cyber-risk environment reasoned that thorough, periodic, and warranted evaluations of the cyber threat posture of the organization assist IT security managers of U.S. government health organizations to identify, analyze, and mitigate security vulnerabilities to employ informed and prudent cyber risk responses.

Based on the data collected, the system and controls development, implementation, and monitoring theme are essential to developing a comprehensive and dynamic cyber defense environment. Nikishova and Vitenburg (2019) state that system security controls selection is dependent upon the protected system or systems, the placement within the enterprise, and the information protection resource and its components to adequately tailor relevant prevention and responses. Systems security or cybersecurity engineering and implementation provide the architecture and design requirements needed to inherently make systems less vulnerable and more resilient to attack or degradation (Hillebrand et al., 2016; McEvilley et al., 2016). Security and privacy assessment plan integrated within the information security strategy of the organization help IT security managers assess implemented security controls for effectiveness according to the organizational strategic objectives (NISTJTF, 2018). As an application to professional practice, assessments of the cyber risk posture of the organization inform cyber control decisions of IT security managers in U.S. government

health institutions on the identification, selection, implementation, and subsequent monitoring of security controls which ensures the efficacy of said controls.

The preponderance of the data collected relevant to the strategy development and coordination through interagency and interdepartmental risk management theme is derived from the consensus of the participants and organizational documentation to implement information sharing at various echelons and strategic-level coordination in terms of cyber risk management. The aforementioned theme holds specific relevance in the healthcare industry concerning its adoption of information technology which has facilitated positive change through automated business processes, enhanced health information sharing, considerably accelerated data processing, and improved overall health organization performance through IT strategic alignment (Alsharif et al., 2018). Data traverses locally, regionally, nationally, and internationally in open exchange digital environments throughout the world (Baldi et al., 2019). This paradigm influences IT security managers of U.S. government health organizations to support and maintain comprehensive, centralized, cooperative, and coordinated cyber risk management strategy as a direct application to professional practice.

Implications for Social Change

The implications for social change concerning this study are directed toward the overarching concept of positively stimulating patient trust and confidence in healthcare systems and strengthening the commitments of healthcare professionals by emphasizing sincere patient privacy. A patient's perception of data security within a U.S. government health organization regarding non-technical and technical protection can notably infer

their trust in a health institution and their perception towards information security (Lo et al., 2018). Patients invest their cognitive and emotional trust in the competence and integrity of healthcare institutions based on the organizational cyber risk strategy, policies, processes, and procedures, determining the degree to which patients depend on the capability of the organization to optimally addresses cyber risk and patient data management (Esmaeilzadeh, 2020). The four overarching themes are derived from the research: structured, systematic, and timely cyber risk management; continuous and consistent assessment of the risk environment; system and controls development, implementation, and monitoring; and strategy coordination through centralized interagency and interdepartmental risk management, inherently have the second-order effect of highlighting custodial responsibilities regarding patient data and patient trust in the capabilities of the organization to safeguard that data. Patient trust in the capabilities of the organization and relevant processes and procedures regarding patient privacy are products of a leap of faith taken by said stakeholders, accepting calculated uncertainty and a degree of risk that organizational strategy will act in good faith on behave of patient data security (Balmer et al., 2020). As consideration for social change implications, the data collected throughout this study suggests that universal benefits regarding the achievement of patient trust and confidence in healthcare systems and data security are directly related to patient awareness of organizational cyber risk strategy efficacy. This efficacy is inherently demonstrated through the employment of controls that successfully resist and disable security breach attempts and requires a particular level of transparency

to patients and healthcare staff regarding organizational strategy and privacy policies to reinforce patient trust and confidence in a presumably competent healthcare system.

Recommendations for Action

The purpose of this qualitative multiple case study was to explore the cybersecurity risk management strategies effectively used by IT security managers to safeguard PHI and PII from data breaches concerning U.S. government health organizations. Rogers (1975) explored the PMT as the outcomes of fear appeals on attitude change and examined influencing factors associated with appropriate courses of action to prevent the noxious occurrence. He determined that there are three components of the PMT that appeal to the natural fear of unfavorable outcomes described as (a) the magnitude of adversity of a depicted event, (b) the event's probability of occurrence, and (c) the effectiveness of a protective response (Rogers, 1975). Using the aforementioned theory as a guide, the four predominant themes developed from data collected for this study: structured, systematic, and timely cyber risk management; continuous and consistent assessment of the risk environment; system and controls development, implementation, and monitoring; and strategy coordination through centralized interagency and interdepartmental risk management, work coupled with the PMT as a framework for action-based considerations. As such, there are a few recommendations for IT security managers to put into action regarding initiation, planning, implementing and executing, monitoring and assessing, and documenting the aforementioned strategies subject to each health institution.

The first recommendation for action is for IT security managers to ensure that the health organization is effectively-prepared to sufficiently respond to the organizational cyber risk environment. Steps to ensuring fruition of this type of preparation can include assigning appropriate and relevant cyber risk-oriented roles and responsibilities, cognizing the mission of the organization concerning prioritizing and insulating critical assets, understanding the threat environment and the associated risk tolerance level of the organization, and identifying or leveraging key stakeholders of the organization (NISTJTF, 2018). The data collected throughout this study has supported the need for IT security managers to enable the most optimal response to cyber risks throughout various echelons of the organization. IT security managers can influence this optimal response strategically using risk management strategy, organizational policies, and procedures conducive to addressing risk from an organizational perspective and achieving governance. IT security managers can also influence optimal cyber risk responses from an operational standpoint and ensuring risk is adequately addressed from the business process level. Finally, the IT security practitioner may influence optimal cyber risk from a tactical level by ensuring risk decisions from the strategic and operational levels are carried out and ensuring the right people with the right responsibilities are in place to identify, analyze, and respond to cyber threats. Johnson et al. (2016) concluded that cybersecurity skills, retention of skills, and adequate roles and responsibilities are growing concerns in U.S.-based organizations, which emphasizes that senior leaders identify and assign roles accordingly to balance strategic objectives and operational and

tactical requirements. This recommendation is supported by adopting a structured, systematic, and timely approach to methodical cyber risk management strategy.

The second recommendation petitions for IT security managers to recognize the volatile nature of the cyber threat environment and proportionally and dynamically adjust organizational cybersecurity approaches based on continuous and consistent assessments of the risk environment. Rwelamila (2016) elaborated on risk process development, stating that the risk assessment, which is divided into risk analysis and risk prioritization, follows risk identification and is statistically more often focused on qualitative risk over quantitative. Emmerich et al. (2016) expanded stating that identifying and analyzing risks of the organization leads to adopting specialized control sets developed for organization-wide use which are directed by requirements engineering. A combination of the reviewed literature, input from the study participants, associated organizational documentation throughout this study has reflected that IT security managers may accomplish this recommendation by implementing periodic and event-based cyber risk assessments to identify potential impacts that threaten critical assets and data exchanges of the health organization. Identification and assessment of potential cyber risk impacts of the health organization as they pertain to the organizational cyber threat environment have the potential to assist IT, security managers, to build comprehensive capabilities and engineering resilience indicative of effective responses and safeguarding assets.

The third recommendation revolves around applying expert judgment from key stakeholders and employing organizationally relevant assessments and other documentation based on analysis of the cyber risk and cyber threat environments. This

recommendation may be achieved through the methodic development, implementation, and systematic monitoring of cybersecurity controls to protect critical assets and data exchanges of the health organization. IT security managers of government health organizations may benefit from methodical selection, implementation, and monitoring for the efficacy of physical, administrative, and technical security controls as they pertain to controlling operational impacts inherent within a cyber risk environment. Fuchs et al. (2016), NISTJTF (2018), and Small and Wainwright (2018) expanded on this concept stating that IT security controls multi-methodology described the identification of business strategies, objectives, and problem definitions used as inputs into the controls selection process and yields the output of relevant controls selection for the organization. Considering security control implementation, there is a need for IT, security managers, to integrate the key processes of availability management (to ensure information availability), IT service continuity management (to ensure information risk reduction and recovery), and incident management (to ensure minimal adverse impacts on the organization and the systems and services are restored quickly) (Belaissaoui & Elkhannoubi, 2015; Herath & Rao, 2009; Keenan et al., 2016; Monken et al., 2017). Farrell (2016) elaborates that once identified changes are formally proposed and reviewed, the changes are then analyzed for any impact to the security of the organization, tested, approved by senior management, and implemented and documented by IT security managers. Security and privacy assessment plan integrated within the information security strategy of the organization help IT security managers assess

implemented security controls for effectiveness according to the organizational strategic objectives (NISTJTF, 2018).

Throughout this study, the literature and associated data collected highlighted that the organizational stewardship of patient data privacy is a product of methodical selection, strategic placement, and periodic assessment of cyber risk-oriented security controls to physically, technically, and administratively or logically safeguard assets of the health organization. Some senior-level IT security managers relevant to this study have benefited from selecting and implementing security controls based on the classification of the data, existing baselines of compliance, the impact level if a cyber threat were realized, and tailored governance. The PMT, as the conceptual framework of this study, outlines these considerations as understanding the consequences of realized risk, the probability of a risk occurrence, and the effectiveness of the response from implemented controls (Rogers, 1975). This recommendation is contingent upon intrinsic and well-defined certification and accreditation processes of selected security controls, industry best practices, and the strategic direction of the organization.

The last recommendation for action is for IT security managers at senior levels to influence the coordination of risk management strategy through centralized interagency and interdepartmental risk management as it pertains to cybersecurity. Moeini and Rivard (2019) propose adopting a strategy that focuses on the indirect influence and relationships of perceived risk exposure and IT project manager mediation and concludes that risk response attitudes are mostly influenced by risk-based decisions. As such, steps to achieving this strategy would focus on documenting and sharing assessment results with

senior leadership within the U.S. government health industry to influence an enduring common understanding of the security and privacy posture throughout each participating health organization (Adato, 2017; Diehl et al., 2016; Ellingson et al., 2017; NISTJTF, 2018).

The research conducted regarding this study focused on understanding the successful organizational strategy implemented by IT security managers that achieves effective cybersecurity. Evidenced through this research was the need of leveraging communal attitudes toward developing a shared level of understanding regarding the cyber threat and cyber risk environment relevant from a government health industry perspective. This recommendation is based on the literature and data collected throughout this study which highlight that shared information throughout the industry as it pertains to the cyber environment empowers health organizations with the ability to forecast relevant cyber threats and dynamically adjust controls accordingly.

IT security managers would inherently action the aforementioned recommendations. However, the organization as a whole should observe enduring benefits from each implemented recommendation, notwithstanding the support of consistent and continual due diligence. A summarization of the finding of this study will be shared with the participants of this study. As this study is formally published through Walden University to the ProQuest database, interested parties will also be able to view the contents of this study based on the achievement of cybersecurity strategy through risk management-based activities performed by IT security managers in U.S. government health organizations. I will also share the findings of this study through conferences or

courses which I am invited to speak and as a training aid or research documentation for those who are wishing to further their independent research in the fields of cybersecurity and risk management.

Recommendations for Further Research

Researchers may consider some fundamental avenues of approach considering future research based on the content of this study and the limitations therein. The targeted population consisted of eight IT security managers of four medium-sized government health institutions located in the mid-west region of the United States. Researchers may find benefit in researching a larger or disassociated population to gain a fuller or more distinct perspective outside of the population size or location-based scope of this study.

Moreover, I used remote methods to conduct interviews; observations; organizational documentation reviews; policy, procedures, and supporting literature reviews as the primary method of data collection for this qualitative multiple case study. However, researchers may find a benefit in conducting onsite data collection as a method to observe storage and access to organizational documentation within a natural setting. Also, researchers may find benefit in future research data collection concerning the content of this study using face-to-face interviews to observe facial expressions, body language, and other nonverbal communication.

Finally, I chose to use a qualitative research methodology coupled with a multiple case study design as the most appropriate approach to explore my research. However, researchers may find benefit in exploring this research using a different methodology or design to gain a different perspective of this research. For example, using a quantitative

or mixed methods methodology to explore this research could lead to understanding how numerical values or variable relationships in a controlled environment impact or alter findings comparatively to this study and therefore developing a new perspective.

Reflections

I have studied, worked, lived, and breathed various aspects of information technology for decades and undoubtedly, for all of my adult life. Although I have previously explored many IT-based topics both scholastically and through an alignment of professional interests, I have not truly experienced the essence of investigative research as I have in developing this study. My experience in conducting this research within the scope of the DIT doctoral study processes has broadened my perspective and has kept me engaged while achieving new personal levels of exploratory research and analysis.

My student colleagues, instructors, committee members, and staff at Walden University have played a vital role in helping me grow as a researcher. Their constructive and supportive feedback has greatly assisted me in avoiding bias and developing and refining this study into an organized and logically sound document. I have learned a great deal through this experience, not only about my subject of study and information technology in general but also about the associated processes and framework of research.

The data collection process and the participant solicitation process subject to this study within the constraints of a pandemic was an unquestionable challenge. However, I am truly thankful that those challenges were overcome and the study participants were identified, involved, and able to help me refine my interpretation of their input through

member checking. The research questions, conceptual framework, and literature review provided a sound foundation of support to guide my research and shape my interpretation of the data collected.

My experience in researching this study has been nothing short of rewarding. I have gained valuable knowledge and lessons learned through this experience. I will use the new skills that I have learned from the development of this study to enhance my craft, further investigate information technology topics of interest, advance the industry, and continue to contribute to positive social change.

Conclusion

This qualitative multiple case study, integrating eight participants and the organizational documentation of four medium-sized government health institutions of mid-west U.S., was developed to explore the cybersecurity risk management strategies used by IT security managers to safeguard PHI and PII from data breaches concerning U.S. government health organizations. Each participant subject to this study was qualified based on their breadth of experience with risk-based cybersecurity adoption and performing cyber-oriented risk management operations. The organizational documentation consisted of enterprise cybersecurity strategies, policies, standards, procedures, regulatory guidance, and other historical documentation and industry-based governance. The PMT was used as the conceptual framework to guide this study along with relevant and supportive research from the literature review.

Developed from data collected for this study, were four predominant themes: (a) structured, systematic, and timely cyber risk management; (b) continuous and consistent

assessment of the risk environment; (c) system and controls development, implementation, and monitoring; and (d) strategy coordination through centralized interagency and interdepartmental risk management. Relevant to the application to professional practice, the aforementioned themes of this study illustrate industry trends that reflect a specific emphasis on the application of risk management concepts as they relate to disabling events leading to data security breaches. The recommendations for IT security managers based on the findings of this study are: (a) ensuring the health organization is adequately prepared to respond to organizational cyber risk through the optimal codification of organizational architecture and maintaining an understanding of the cyber threat and cyber risk environment, (b) proportionally and dynamically select and implement cybersecurity controls based on continuous and consistent assessments of the risk environment, (c) applying expert judgment to employ organizationally relevant baselines and assessments to actively monitor and evaluate the efficacy of cybersecurity controls, (d) and influencing the coordination of risk management strategy through centralized interagency and interdepartmental risk management processes as they pertain to organizational cybersecurity. The findings of this study may contribute knowledgebase of IT security managers, overall IT best practices, and positive social change.

References

Abercrombie, R. K., Haney, M., Jillepalli, A. A., Leon, D. C., & Sheldon, F. T. (2017). Security management of cyber physical control systems using NIST SP 800-82r2. *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC).* Gaithersburg: NIST. https://doi.org/10.1109/IWCMC.2017.7986568

Abie, H., & Boudko, S. (2019). Adaptive cybersecurity framework for healthcare internet of things. *IEEE Proceedings: 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT).* Oslo: IEEE. https://doi.org/10.1109/ISMICT.2019.8743905

Abler, L., Khoza, N., MacPhail, C., & Ranganathan, M. (2016). Process guidelines for establishing intercoder reliability in qualitative studies. *Qualitative Research, 16*(2), 198-212. https://doi.org/10.1177/1468794115577012

Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. *Business Horizons, 62*(4), 539-548. https://doi.org/10.1016/j.bushor.2019.03.010

Abramson, C. M., Dohan, D., Garrett, S. B., Halley, M. C., & Rendle, K. A. (2019). Beyond exploratory: A tailored framework for designing and assessing qualitative health research. *BMJ Open, 9*(8). https://doi.org/10.1136/bmjopen-2019-030123

Adashi, E. Y., Menikoff, J. A., & Walters, L. B. (2018). The Belmont Report at 40: Reckoning with time. *American Journal of Public Health, 108*(10), 1345-1348. https://doi.org/10.2105/AJPH.2018.304580

Adato, L. (2017). Monitoring and automation: It's easier than you think. *Network Security, 2017*(4), 5-7. https://doi.org/10.1016/S1353-4858(17)30036-3

Adni, T., Martin, K., & Mudge, E. (2012). The psychosocial impact of chronic wounds on patients with severe epidermolysis bullosa. *Journal of Wound Care, 21*(11), 528-536. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=rzh&AN=104245087&site=eds-live&scope=site

Aguinis, H., Brutus, S., & Wassmer, U. (2013). Self-reported limitations and future directions in scholarly reports: Analysis and recommendations. *Journal of Management, 39*(1), 48-75. https://doi.org/10.1177/0149206312455245

Ahmad, Z., Liew, T. H., Norhashim, M., & Ong, T. S. (2019). Security monitoring and information security assurance behavior among employees: An empirical analysis. *Information & Computer Security, 27*(2), 165-188. https://doi.org/10.1108/ICS-10-2017-0073

Ahmed, Y., Joephs, M., & Nadqvi, S. (2019). Cybersecurity metrics for enhanced protection of healthcare IT systems. *IEEE Proceedings: International Symposium on Medical Information and Communication Technology (ISMICT)* (pp. 1-9). Birmingham City: IEEE. https://doi.org/10.1109/ISMICT.2019.8744003

Ahriz, S., Illousamen, E. H., Mansouri, K., Qbadou, M., & Yamami, A. E. (2017). Representing IT projects risk management best practices as a metamodel. *Engineering Technology & Applied Science Research, 7*(5), 2062-2067. https://search-ebscohost-

com.ezp.waldenulibrary.org/login.aspx?direct=true&db=edb&AN=125774886&site=eds-live&scope=site

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. *Action Control: From Cognition to Behavior*, 11-39. https://doi.org/10.1007/978-3-642-69746-3_2

Alam, R. G., & Ibrahim, H. (2019). Cybersecurity strategy for smart city implementation. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences. XLII-4-W17*, pp. 3-6. Copernicus Publications. https://doi.org/10.5194/isprs-archives-XLII-4-W17-3-2019

Alaydrus, M., Nugraha, B., & Purwanti, S. (2017). Enhancing security on E-health private data using SHA-512. *IEEE Proceedings: 2017 International Conference on Broadband Communication, Wireless Sensors and Powering (BCWSP).* Jakarta: IEEE. https://doi.org/10.1109/BCWSP.2017.8272557

Aldya, A. P., Rosmansyah, Y., & Sutikno, S. (2019). Measuring effectiveness of control of information security management system based on SNI ISO/IEC 27004: 2013 standard. *IOP Conference Series: Materials Science and Engineering, 550*(1), 1-1. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=edb&AN=138490756&site=eds-live&scope=site

Alexander, A., & Cummings, J. (2016). The rise of the chief information security officer. *People & Strategy, 39*(1), 10-13. https://search-ebscohost-

com.ezp.waldenulibrary.org/login.aspx?direct=true&db=bth&AN=112590898&site=eds-live&scope=site

Aljohani, N. R., Daud, A., Dawood, H., Masood, I., & Wang, Y. (2018). Towards smart healthcare: Patient data privacy and security in sensor-cloud infrastructure. *Wireless Communications & Mobile Computing*, 1-23. https://doi.org/10.1155/2018/2143897

Almeida, F., Carvalho, I., & Cruz, F. (2018). Structure and challenges of a security policy on small and medium enterprises. *KSII Transactions on Internet and Information Systems, 12*(2), 747-763. https://doi.org/10.3837/tiis.2018.02.012

Alpi, K. M., & Evans, J. J. (2019). Distinguishing case study as a research method from case reports as a publication type. *Journal of the Medical Library Association, 107*(1), 1-5. https://doi.org/10.5195/jmla.2019.615

Alsharif, S., Benslimane, N., Khalifa, M., & Price, C. (2018). Healthcare IT strategic alignment: Challenges and recommendations. *Studies in Health Technology & Informatics, 251*, 207-210. https://doi.org/10.3233/978-1-61499-880-8-207

Alshawish, A., De Meer, H., & Spielvogel, K. (2019). A model-based time-to-compromise estimator to assess the security posture of vulnerable networks. *2019 International Conference on Networked Systems (NetSys) Networked Systems (NetSys).* Munich: IEEE. https://doi.org/10.1109/NetSys.2019.8854511

Amankwaa, L. (2016). Creating protocols for trustworthiness in qualitative research. *Journal of Cultural Diversity, 23*(3), 121-127. https://search-ebscohost-

com.ezp.waldenulibrary.org/login.aspx?direct=true&db=rzh&AN=118362617&site=eds-live&scope=site

Ames, H., Glenton, C., & Lewin, S. (2019). Purposive sampling in a qualitative evidence synthesis: a worked example from a synthesis on parental perceptions of vaccination communication. *BMC Medical Research Methodology, 19*(1), 1-9. https://doi.org/10.1186/s12874-019-0665-4

Ammenwerth, E., & Leber, S. (2017). Identification of measures and indicators for the IT security of networked medical devices: A Delphi study. *Studies in Health Technology And Informatics, 243*, 141-151. https://ezp.waldenulibrary.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=mnh&AN=28883189&site=eds-live&scope=site

Anderson, B. R., Cowley, J. A., & Nauer, K. S. (2015). Emergent relationships between team member interpersonal styles and cybersecurity team performance. *Procedia Manufacturing. 3*, pp. 5110-5117. Elsevier B. V. https://doi.org/10.1016/j.promfg.2015.07.526

Anderson, D., & Manson, S. (2019). Cybersecurity for protection and control systems: An overview of proven design solutions. *IEEE Industry Applications Magazine, 25*(4), 14-23. https://doi.org/10.1109/MIAS.2018.2875175

Arain, M. A., Birney, A., Hepp, S. L., & Tarraf, R. C. (2017). Evaluation of the awareness and effectiveness of IT security programs in a large publicly funded health care system. *Health Information Management Journal, 47*(3), 116-124. https://doi.org/10.1177/1833358317722038

Arantzamendi, M., Díez-Del-Corral, M. P., Errasti-Ibarrondo, B., & Jordán, J. A. (2018). Conducting phenomenological research: Rationalizing the methods and rigor of the phenomenology of practice. *Journal of Advanced Nursing, 74*(7), 1723-1734. https://doi.org/10.1111/jan.13569

Aromataris, E., Lockwood, C., Munn, Z., Pearson, A., & Porritt, K. (2014). Establishing confidence in the output of qualitative research synthesis: the ConQual approach. *BMC Medical Research Methodology, 14*(1), 108-114. https://doi.org/10.1186/1471-2288-14-108

Arsel, Z. (2017). Asking questions with reflexive focus: A tutorial on designing and conducting interviews. *Journal of Consumer Research, 44*(4), 939-948. https://doi.org/10.1093/jcr/ucx096

Atkins, L., Cole, C., & Mitri, M. (2017). Teaching case a systems analysis role-play exercise and assignment. *Journal of Information Systems Education, 28*(1), 1-9. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=eue&AN=126157284&site=eds-live&scope=site

Awan, M. S., Burnap, P., Javed, A., & Rana, O. (2015). Continuous monitoring and assessment of cybersecurity risks in large computing infrastructures. *IEEE Proceedings* (pp. 1442–1447). New York: IEEE. https://doi.org/10.1109/HPCC-CSS-ICESS.2015.224

Aziz, A., Laken, M., Lenert, L., Marshall, E., Obeida, J., Qanungo, S., & Welch, B. (2016). Teleconsent: A novel approach to obtain informed consent for research.

Contemporary Clinical Trials Communications, 3, 74-79. https://doi.org/10.1016/j.conctc.2016.03.002

Babbage, D. R., Farris, A. J., Lowe, A., & Norris, A. C. (2018). Quantifying thematic saturation in qualitative data analysis. *Field Methods, 30*(3), 191-207. https://doi.oeg/10.1177/1525822X17749386

Bailey, D., Dempsey, K., Gupta, S., Johnson, A., & Ross, R. (2011). Guide for security-focused configuration management of information systems. *NIST Special Publication, 800-128*, 1-99. https://doi.org/10.6028/NIST.SP.800-128

Baldi, M., Chiaraluce, F., Gottardi, G., & Santini, P. (2019). A data-driven approach to cyber risk assessment. *Security and Communication Networks, 2019*, 1-8. https://doi.org/10.1155/2019/6716918

Baldini, G., Hernández-Ramos, J. L., Matheu-García, S. N., & Skarmeta, A. F. (2019). Risk-based automated assessment and testing for the cybersecurity certification and labeling of IoT devices. *Computer Standards & Interfaces, 62*, 64-83. https://doi.org/10.1016/j.csi.2018.08.003

Balmer, A., Cheeks, C., Davidson, S., Devereux, J., Findlay, D., Friesen, P., . . . Sheehan, M. (2020). Trust, trustworthiness and sharing patient data for research. *Journal of medical ethics*. https://doi.org/10.1136/medethics-2019-106048

Bamberg, M., Creswell, J. W., Frost, D. M., Josselson, R., Levitt, H. M., & Suárez-Orozco, C. (2018). Journal article reporting standards for qualitative primary, qualitative meta-analytic, and mixed methods research in psychology: The APA

publications and Communications Board Task Force report. *American Psychologist, 73*(1), 26-46.

Bansal, P., Smith, W. K., & Vaara, E. (2018). New ways of seeing through qualitative research. *Academy of Management Journal, 61*(4), 1189-1195, 7. https://doi.org/10.5465/amj.2018.4004

Baronienė, L., & Žirgutis, V. (2017). Cybersecurity facets: Counterfactual impact evaluation of measure "Procesas LT" in enterprises of the IT sector. *Journal of Security & Sustainability Issues, 6*(3), 445-456. https://doi.org/10.9770/jssi.2017.6.3(10)

Bartol, N., Boyens, J., Paulsen, C., & Winkler, K. (2018). Criticality analysis process model: Prioritizing systems and components. *NIST*, 1-94. https://doi.org/10.6028/NIST.IR.8179

Basile, C., Ceccato, M., Coppens, B., De Sutter, B., Falcarin, P., Tonella, P., & Torchiano, M. (2017). How professional hackers understand protected code while performing attack tasks. *IEEE Proceedings: 2017 IEEE/ACM 25th International Conference on Program Comprehension (ICPC), Program Comprehension (ICPC)* (pp. 154-164). Buenos Aires: IEEE. https://doi.org/10.1109/ICPC.2017.2

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. *Qualitative Report, 13*(4), 544-559. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=eric&AN=EJ824836&site=eds-live&scope=site

Beail, N., & Williams, K. (2014). Using qualitative methods in research with people who have intellectual disabilities. *Journal of Applied Research in Intellectual Disabilities, 27*(2), 85–96. https://doi.org/10.1111/jar.12088

Belaissaoui, M., & Elkhannoubi, H. (2015). A framework for an effective cybersecurity strategy implementation: Fundamental pillars identification. *IEEE Proceedings: 2015 15th International Conference on Intelligent Systems Design and Applications (ISDA)* (pp. 1-6). Marrakech: IEEE. https://doi.org/10.1109/ISDA.2015.7489156

Beretvas, S. N., Ferron, J. M., Moeyaert, M., Ugille, M., & Van den Noortgate, W. (2014). The influence of the design matrix on treatment effect estimates in the quantitative analyses of single-subject experimental design research. *Behavior Modification, 38*(5), 665-704. https://doi.org/10.1177/0145445514535243

Bernard, R. (2013). *Social research methods: Qualitative and quantitative approaches* (2nd ed.). Thousand Oaks: Sage.

Bero, L. (2017). Addressing bias and conflict of interest among biomedical researchers. *JAMA, 317*(17), 1723-1724. https://doi.org/10.1001/jama.2017.3854

Berta, W. B., Gagliardi, A. R., & Zych, M. M. (2019). Initiation is recognized as a fundamental early phase of integrated knowledge translation (IKT): qualitative interviews with researchers and research users in IKT partnerships. *BMC Health Services Research, 19*(1), 1-10. https://doi.org/10.1186/s12913-019-4573-4

Birkinshaw, C., Rouka, E., & Vassilakis, V. G. (2019). Implementing an intrusion detection and prevention system using software-defined networking: Defending

against port-scanning and denial-of-service attacks. *Journal of Network and Computer Applications, 136*, 71-85. https://doi.org/10.1016/j.jnca.2019.03.005

Birt, L., Campbell, C., Cavers, D., Scott, S., & 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

Biskupek, A. (2018). Risk management in IT projects - case study. *Trendy Ekonomiky a Managementu, 12*(32), 21-33. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=edb&AN=138290036&site=eds-live&scope=site

Blair, J. R., Hall, A. O., & Sobiesk, E. (2019). Educating future multidisciplinary cybersecurity teams. *Computer (New York), 52*(3), 58-66. https://doi.org/10.1109/MC.2018.2884190

Böcher, M., Krott, M., & Nagasaka, K. (2016). Are forest researchers only scientists? Case studies on the roles of researchers in Japanese and Swedish forest policy processes. *Forest Policy and Economics, 70*, 147-154. https://doi.org/10.1016/j.forpol.2016.06.006

Bohme, R., & Laube, S. (2017). Strategic aspects of cyber risk information sharing. *ACM Computing Surveys, 50*(5), 1-77. https://doi.org/10.1145/3124398

Bonfils, K. A., Firmin, R. L., Luther, L., Minor, K. S., & Salyers, M. P. (2017). Using text-analysis computer software and thematic analysis on the same qualitative data: A case example. *Qualitative Psychology, 4*(3), 201-210. https://doi.org/10.1037/qup0000050

Boonjing, V., & Pimchangthong, D. (2017). Effects of risk management practice on the success of IT project. *Procedia Engineering, 182*, 579-586. https://doi.org/10.1016/j.proeng.2017.03.158

Bouikidis, C. D., & Rutberg, S. (2018). Exploring the evidence. Focusing on the fundamentals: A simplistic differentiation between qualitative and quantitative research. *Nephrology Nursing Journal, 45*(2), 209-213. https://eds-a-ebscohost-com.ezp.waldenulibrary.org/eds/pdfviewer/pdfviewer?vid=6&sid=715aa42a-d853-4572-932c-10092bd8c8bd%40sessionmgr4009

Boyle, S., Reaiche, C., & Torten, R. (2018). The impact of security awareness on information technology professionals' behavior. *Computers & Security, 79*, 68-79. https://doi.org/10.1016/j.cose.2018.08.007

Boz, H., & Daglı, Y. (2017). The contribution of qualitative methods for identifying the educational needs of adults. *Cypriot Journal of Educational Sciences, 12*(4), 167-176. https://files.eric.ed.gov/fulltext/EJ1166509.pdf

Bradshaw, M. (2002). Contracts and member checks in qualitative research in human geography: Reason for caution? *Area, 33*(2), 202-211. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=edb&AN=19957436&site=eds-live&scope=site

Brilingaitė, A., Bukauskas, L., & Juozapavičius, A. (2019). A framework for competence development and assessment in hybrid cybersecurity exercises. *Computers & Security, 88*. https://doi.org/10.1016/j.cose.2019.101607

Buttell, F., & Cannon, C. (2015). Institutional review boards at very high research activity universities: An opportunity for social workers. *Research on Social Work Practice, 25*(7), 832-835. https://doi.org/10.1177%2F1049731514557699

Cagliano, A. C., Grimaldi, S., & Rafele, C. (2015). Choosing project risk management techniques. A theoretical framework. *Journal of Risk Research, 18*(2), 232-248. https://doi.org/10.1080/13669877.2014.896398

Cao, Z., Jiang, S., & Zhang, X. (2019). An improved Leaderrank algorithm for identifying critical components in service-oriented systems. *Journal of Physics: Conference Series, 1213*(2019). https://doi.org/10.1088/1742-6596/1213/3/032012

Carr, L. T. (1994). The strengths and weaknesses of quantitative and qualitative research: what method for nursing? *Journal of Advanced Nursing, 20*(4), 716-721. https://doi.org/10.1046/j.1365-2648.1994.20040716.x

Casey, B., Corbally, M., & Proudfoot, D. (2016). Narrative in nursing research: an overview of three approaches. *Journal of Advanced Nursing, 72*(5), 1203-1215. https://doi.org/10.1111/jan.12887

Center for Internet Security. (2019). *The 20 CIS controls and resources.* https://www.cisecurity.org/controls/cis-controls-list/

Cenys, A., Goranin, N., Janulevicius, J., Kaceniauskas, A., & Olifer, D. (2019). Defining the minimum security baseline in a multiple security standards environment by graph theory techniques. *Applied Sciences, 9*(4), 681. https://doi.org/10.3390/app9040681

Chakravarthy, K., Chaturvedi, & Williams, C. (2020). Cybersecurity risks in a pandemic. *Journal of medical Internet research, 22*(9). https://doi.org/10.2196/23692

Chen, Q., Dai, T., Hu, H., & Li, J. (2017). Research of China's general hospital informationization construction situation. *Biomedical Research (0970-938X), 28*(20), 8583-8593. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=a9h&AN=127337210&site=eds-live&scope=site

Chen, Y.-H., Chou, T.-C., & Yang, C. (2019). Bridging digital boundary in healthcare systems: An interoperability enactment perspective. *Computer Standards & Interfaces, 62*, 43-52. https://doi.org/10.1016/j.csi.2018.08.001

Clapper, D., & Richmond, W. (2016). Small business compliance with PCI DSS. *Journal of Management Information & Decision Sciences, 19*(1), 54-67. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=bth&AN=125770626&site=eds-live&scope=site

Clark, K. (2019). Ethics in research. *Radiologic Technology, 90*(4), 394-397. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=rzh&AN=134820187&site=eds-live&scope=site

Clark, K. R., & Vealé, B. L. (2018). Strategies to enhance data collection and analysis in qualitative research. *Radiologic Technology, 89*(5), 482CT-485CT. https://search-ebscohost-

com.ezp.waldenulibrary.org/login.aspx?direct=true&db=rzh&AN=129386154&site=eds-live&scope=site

Cohen, O., Boyd, J. E., Denzinger, J., & Thornton, C. (2015). Automated testing of physical security: Red teaming through machine learning. *Computational Intelligence*. https://doi.org/10.1111/coin.12034

Cole, P., & Harper, M. (2012). Member checking: Can benefits be gained similar to group therapy? *The Qualitative Report, 17*(2), 510-517. https://nsuworks.nova.edu/tqr/vol17/iss2/1

Collard, G., Disson, E., Ducroquet, S., & Talens, G. (2017). A definition of information security classification in cybersecurity context. *IEEE Proceedings: 2017 11th International Conference on Research Challenges in Information Science (RCIS)* (pp. 77-82). Brighton: IEEE. https://doi.org/10.1109/RCIS.2017.7956520

Connolly, M., Mackieson, P., & Shlonsky, A. (2019). Increasing rigor and reducing bias in qualitative research: A document analysis of parliamentary debates using applied thematic analysis. *Qualitative Social Work, 18*(6), 965-980. https://doi.org/10.1177%2F1473325018786996

Considine, B., Janvrin, D. J., Krahel, J. P., & Lenk, M. M. (2019). Social technology: An integrated strategy and risk. *The Journal of Information Systems, 33*(2), 129-153. https://doi.org/10.2308/isys-52065

Cope, D. G. (2014). Methods and meanings: Credibility and trustworthiness of qualitative research. *Oncology Nursing Forum, 41*(1), 89-91. https://doi.org/10.1188/14.ONF.89-91

Cortelyou-Ward, K., Gabriel, M. H., Noblin, A., Rutherford, A., & Walden, A. (2018). Data breach locations, types, and associated characteristics among US hospitals. *American Journal of Managed Care, 24*(2), 78-84. https://www.ajmc.com/journals/issue/2018/2018-vol24-n2/data-breach-locations-types-and-associated-characteristics-among-us-hospitals

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems, 26*(6), 605-641. https://doi.org/10.1057/s41303-017-0059-9

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches.* Thousand Oaks: Sage Publications.

Cybersecurity Information Sharing Act of 2015, S. 2588 S.754 (2015). https://www.congress.gov/bill/114th-congress/senate-bill/754

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

Davidoff, S. (2017). Cybersecurity audits getting to good. *GP Solo, 34*(4), 56-59. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=a9h&AN=124656529&site=eds-live&scope=site

Deakin, H., & Wakefield, K. (2014). Skype interviewing: Reflections of two PhD researchers. *Qualitative Research*, 603-616. https://doi.org/10.1177/1468794113488126

DeCino, D. A., & Waalkes, P. L. (2019). Aligning epistemology with member checks. *International Journal of Research & Method in Education, 42*(4), 374-384. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=edb&AN=137679907&site=eds-live&scope=site

Denning, P. J., & Lewis, T. G. (2018). Learning machine learning. *Communications of the ACM, 61*(12), 24-27. https://doi.org/10.1145/3286868

Denzin, N. K., & Lincoln, Y. S. (2018). *The Sage handbook of qualitative research* (5th ed.). Los Angeles, California: Sage Publications.

Devadas, B. (2016). A critical review of qualitative research methods in evaluating nursing curriculum models: Implication for nursing education in the Arab world. *Journal of Education and Practice, 7*(7), 119-126. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=eric&AN=EJ1095296&site=eds-live&scope=site

Diefenbach, M. A., Duhamel, K., Nelson, C. J., Saracino, R. M., & Tutino, R. (2019). Participant recruitment strategies in psychosocial oncology research: A comparison of in-person and telephone approaches. *Journal of Psychosomatic Research, 125*, N.PAG-N.PAG. https://doi.org/10.1016/j.jpsychores.2019.109817

Diehl, L. L., Friedberg, S. C., Hayes, G. C., Hepp, P. E., & Meade, M. (2016). Attacking cybersecurity from the inside out. *Journal of Health Care Compliance, 18*(6), 33-36. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=bth&AN=120089255&site=eds-live&scope=site

Drake, M., & Jervis, M. (2014). The use of qualitative research methods in quantitative science: A review. *Journal of Sensory Studies, 29*(4), 234-247. https://doi.org/10.1111/joss.12101

Du, L., Deng, Z., Lu, G., Ma, J., Xia, C., & Xia, S. (2018). A machine learning based approach to identify protected health information in Chinese clinical text. *International Journal of Medical Informatics, 116*, 24-32. https://doi.org/10.1016/j.ijmedinf.2018.05.010

Duan, Q., Rawal, B., Wang, Y., & Zhang, P. (2017). Usability and security go together: A case study on database. *IEEE Proceedings: 2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM)* (pp. 49-54). Tindivanam: IEEE. https://doi.org/10.1109/ICRTCCM.2017.86

Dzhafarov, E. N. (2019). On universality of classical probability with contextually labeled random variables: Response to A. Khrennikov. *Journal of Mathematical Psychology, 89*, 93-97. https://doi.org/10.1016/j.jmp.2018.12.002

Edenharter, G., Emmert, M., Griensven, M. v., Pförringer, D., Santarpino, G., Seidl, F., & Vogt, F. (2018). Healthcare IT utilization and penetration among physicians:

Novel IT solutions in healthcare – use and acceptance in hospitals. *European Surgical Research, 59*(1-2), 100-113. https://doi.org/10.1159/000490241

Ellingson, D., Kahle-Piasecki, L., & Ritzman, M. E. (2017). Up in the cloud: Managers, employees, and security training for cloud computing to avert cyber threats. *American Journal of Management, 17*(7), 58-63. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=bth&AN=129961594&site=eds-live&scope=site

Emerson, R. W. (2015). Convenience Sampling, Random Sampling, and Snowball Sampling: How Does Sampling Affect the Validity of Research? *Journal of Visual Impairment & Blindness, 109*(2), 164-168. https://doi.org/10.1177/0145482X1510900215

Emmerich, M., Fernandes, V. B., Janicke, H., Moorsel, A. v., & Yevseyeva, I. (2016). Two-stage security controls selection. *Procedia Computer Science, 100*, 971–978. https://doi.org/10.1016/j.procs.2016.09.261

Ergun, M. (2017). Philosophy of the reliability of qualitative data and interpretation. *Participatory Educational Research*(3), 124-140. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=eue&AN=137788963&site=eds-live&scope=site

Esmaeilzadeh, P. (2020). The effect of the privacy policy of Health Information Exchange (HIE) on patients' information disclosure intention. *Computers & Security, 95*. https://doi.org/10.1016/j.cose.2020.101819

Executive Order 13636. (2013). Improving Critical Infrastructure Cybersecurity. https://obamawhitehouse.archives.gov/the-press-office/2013/02/2012/executive-order-improving-critical-infrastructure-cybersecurity

Farquhar, J., Michels, N., & Robson, J. (2018). Triangulation in industrial qualitative case study research: Widening the scope. *Industrial Marketing Management*. https://doi.org/10.1016/j.indmarman.2020.02.001

Farrell, R. (2016). Regulatory compliance: A change management challenge. *ISSA Journal, 14*(6), 8-31. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=tsh&AN=124183436&site=eds-live&scope=site

Ferrando, M., Hoogerwerf, E.-J., & Kadyrbaeva, A. (2019). Qualitative research on the factors affecting transferability of digital solutions for integrated care. *International Journal of Integrated Care (IJIC), 19*(S1), 1-2. https://doi.org/10.5334/ijic.s3236

FitzPatrick, B. (2019). Validity in qualitative health education research. *Currents in Pharmacy Teaching and Learning, 11*(2), 211-217. https://doi.org/10.1016/j.cptl.2018.11.014

Fountouki, A., & Theofanidis, D. (2018). Limitations and delimitations in the research process. *Journal of Perioperative Nursing, 7*(3), 155-162. https://doi.org/10.5281/zenodo.2552022

Frederick, B., Jacobson, T., Kruse, C. S., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and*

Health Care: Official Journal Of The European Society For Engineering And Medicine, 25(1), pp. 1-10. https://doi.org/10.3233/THC-161263

Freitas, L., Magalhaes, L., Ramos, J., Riberiro, P., & Varajao, J. (2018). Implementing success management in an IT project. *Procedia Computer Science, 138*, 891-898. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=edo&AN=132688764&site=eds-live&scope=site

Fuchs, L., Hummer, M., Kunz, M., Netter, M., & Pernul, G. (2016). Adaptive identity and access management-contextual data based policies. *EURASIP Journal on Information Security, 2016*(1), 1-16. https://doi.org/10.1186/s13635-016-0043-2

Fugini, M., Hadjichristofi, G., & Teimourikia, M. (2016). A web-based cooperative tool for risk management with adaptive security. *Future Generation Computer Systems, 54*, 409-422. https://doi.org/10.1016/j.future.2015.04.015

Fusch, G. E., Fusch, P., & Ness, L. R. (2018). Denzin's paradigm shift: Revisiting triangulation in qualitative research. *Journal of Social Change, 10*(1), 19–32. https://doi.org/10.5590/JOSC.2018.10.1.02

Gan, H., Lau, L., & Yang, L. (2020). Investors' perceptions of the cybersecurity risk management reporting framework. *International Journal of Accounting & Information Management, 28*(1), 167-183. https://doi.org/10.1108/IJAIM-02-2019-0022

Gelleri, P., Gurt, J., Hergert, J., Marcus, B., & Weigelt, O. (2017). The use of snowball sampling for multi source organizational research: Some cause for concern. *Personnel Psychology, 70*(3), 39, 635. https://doi.org/10.1111/peps.12169

Gourisetti, N. G., Mylrea, M., & Patangia, H. (2019). Application of rank-weight methods to blockchain cybersecurity vulnerability assessment framework. *IEEE Proceedings: 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC).* Las Vegas: IEEE. https://doi.org/10.1109/CCWC.2019.8666518

Gregory, P. H. (2017). *CISA certified information systems auditor all-in-one exam guide* (3rd ed.). McGraw-Hill/Osborne.

Grohmann, A. (2018). Evolution of the cybersecurity framework. *ISSA Journal, 16*(7), 14-18. http://search.ebscohost.com/login.aspx?direct=true&AuthType=shib&db=tsh&AN=130572679&site=eds-live&scope=site

Guba, E. G., & Lincoln, Y. S. (1985). *Naturalistic inquiry.* Newbury Park: Sage Publications.

Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations. *Information & Management, 49*(6), 320-326. https://doi.org/10.1016/j.im.2012.08.001

Hadar, E., & Hassanzadeh, A. (2019). Big data analytics on cyber attack graphs for prioritizing agile security requirements. *IEEE Proceedings: 2019 IEEE 27th*

International Requirements Engineering Conference (RE) (pp. 330-339). Jeju Island: IEEE. https://doi.org/10.1109/RE.2019.00042

Haddad, P., Muhammad, I., & Wickramasinghe, N. (2017). Key factors for the successful adoption of IS/IT in healthcare: A fit-viability perspective. *Studies in health technology and informatics, 245*, 1313. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=mnh&AN=29295396&site=eds-live&scope=site

Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management, 33*(1), 2-16. https://doi.org/10.1080/10580530.2015.1117842

Harcourt, D., Heath, J., Williams, L., & Williamson, H. (2018). "It's just more personal": Using multiple methods of qualitative data collection to facilitate participation in research focusing on sensitive subjects. *Applied Nursing Research, 43*, 30-35. https://doi.org/10.1016/j.apnr.2018.06.015

Harvey, L. (2015). Beyond member-checking: A dialogic approach to the research interview. *International Journal of Research & Method in Education, 38*(1), 23-28. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=eric&AN=EJ1049377&site=eds-live&scope=site

Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (1996). https://www.govinfo.gov/content/pkg/PLAW-104publ191/html/PLAW-104publ191.htm

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125. https://doi.org/10.1057/ejis.2009.6

Hickson, H. (2016). Becoming a critical narrativist: Using critical reflection and narrative inquiry as research methodology. *Qualitative Social Work: Research and Practice*, 380-391. https://doi.org/10.1177/1473325015617344

Higginbottom, G. M. (2004). Sampling issues in qualitative research. *Nurse Researcher, 12*(1). https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=edsovi&AN=edsovi.00021768.200412010.00003&site=eds-live&scope=site

Hillebrand, J., Karner, M., Rom, W., Romer, K., & Steger, M. (2016). A security metric for structured security analysis of cyber-physical systems supporting SAE J3061. *IEEE Proceedings: 2016 2nd International Workshop on Modelling, Analysis, and Control of Complex CPS (CPS Data) Modelling, Analysis, and Control of Complex CPS (CPS Data),.* Vienna: IEEE. https://doi.org/10.1109/CPSData.2016.7496425

Hoadley, C., Ince, S., & Kirschner, P. A. (2019). The role of libraries in teaching doctoral students to become information-literate researchers: A review of existing practices and recommendations for the future. *Information and Learning Sciences, 120*(3/4), 158-172. https://doi.org/10.1108/ILS-07-2018-0058

Hu, G., & Wang, H. (2018). Design of message validation method in HL7 medical information system. *IEEE Proceedings: 2018 2nd IEEE Advanced Information*

Management,Communicates, Electronic and Automation Control Conference (IMCEC). Xi'an: IEEE. https://doi.org/10.1109/IMCEC.2018.8469672

Huang, G. C., Jaffe, L. E., Lindell, D., & Sullivan, A. M. (2019). Clear skies ahead: optimizing the learning environment for critical thinking from a qualitative analysis of interviews with expert teachers. *Perspectives on Medical Education*, 289-297. https://doi.org/10.1007/s40037-019-00536-5

Humble, Á., & Radina, E. (2019). *How qualitative data analysis happens: Moving beyond "themes emerged".* New York: Routledge. https://doi.org/10.4324/9781315171647

Iguchi, M. Y., Panicker, S., & Ross, M. W. (2018). Ethical aspects of data sharing and research participant protections. *American Psychologist, 73*(2), 138-145. https://doi.org/10.1037/amp0000240

International Organization for Standardization. (2016). *Information technology - security techniques - information security management - monitoring, measurement, analysis and evaluation.* Geneva: ISO/IEC. https://www.iso.org/standard/64120.html

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: A systematic, organizational perspective. *Journal Of Medical Internet Research, 20*(5), e10059. https://doi.org/10.2196/10059

Javani, B., & Rwelamila., P. M. (2016). Risk management in IT projects: A case of the South African public sector. *International Journal of Managing Projects in Business, 9*(2), 389-413. https://doi.org/10.1108/IJMPB-07-2015-0055

Jayanthi, M. K. (2017). Strategic planning for information security: DID mechanism to befriend the cyber criminals to assure cyber freedom. *IEEE Proceedings: 2017 2nd International Conference on Anti-Cyber Crimes (ICACC) Anti-Cyber Crimes (ICACC)* (pp. 142-147). Abha: IEEE. https://doi.org/10.1109/Anti-Cybercrime.2017.7905280

Jervis, R. (1979). Deterrence theory revisited. *World Politics, 31*(2), 289-324. https://doi.org/:10.2307/2009945

Jobin, P., & Turale, S. (2019). Choosing the right qualitative approach: Is phenomenography a design for my study? *Pacific Rim International Journal of Nursing Research, 23*(4), 314-319.

Johnson, M. E., & Kwon, J. (2015). Protecting patient data: The economic perspective of healthcare security. *IEEE Security & Privacy, 13*(5), 90-95. https://doi.org/10.1109/MSP.2015.113

Johnson, V., Kappelman, L., Maurer, C., McLean, E., Nguyen, Q., Snyder, M., & Torres, R. (2016). The 2016 SIM IT issues and trends study. *MIS Quarterly Executive, 16*(1), 47-80. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=bth&AN=121491407&site=eds-live&scope=site

Jong, J., Ottrey, E., & Porter, J. (2018). Ethnography in nutrition and dietetics research: A systematic review. *Journal of the Academy of Nutrition and Dietetics, 118*(10), 1903-1942. https://doi.org/10.1016/j.jand.2018.06.002

Jurn, J., Kim, H., & Kim, T. (2018). An automated vulnerability detection and remediation method for software security. *Sustainability, 10*(5). https://doi.org/10.3390/su10051652

Karanja, E. (2017). The role of the chief information security officer in the management of IT security. *Information & Computer Security, 25*(3), 300-329. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=edb&AN=124466767&site=eds-live&scope=site

Karasev, S. N., Livshitz, I. I., Lontsikh, P. A., & Nikiforova, K. A. (2016). The new aspects for the instantaneous information security audit. *IEEE Proceedings: 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies (IT&MQ&IS).* Nalchik: IEEE. https://doi.org/10.1109/ITMQIS.2016.7751920

Keenan, F., MacMahon, S. T., & McCaffery, F. (2016). The MedITNet assessment framework: development and validation of a framework for improving risk management of medical IT networks. *Journal of Software: Evolution and Process, 28*(9), 817-834. https://doi.org/10.1002/smr.1782

Kim, Y.-W., Cho, N., & Jang, H.-J. (2018). Trends in research on the security of medical information in Korea: Focused on information privacy security in hospitals. *Healthcare Informatics Research, 24*(1), 61-68. https://doi.org/10.4258/hir.2018.24.1.61

Kirkwood, A., & Price, L. (2013). Examining some assumptions and limitations of research on the effects of emerging technologies for teaching and learning in higher education. *British Journal of Educational Technology, 44*(4), 536-543. https://doi.org/10.111/bjet.12049

Kivunja, C., & Kuyini, A. B. (2017). Understanding and Applying Research Paradigms in Educational Contexts. *International Journal of Higher Education, 6*(5), 26-41. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=eric&AN=EJ1154775&site=eds-live&scope=site

Konradsen, H., Østergaard, B., & Voltelen, B. (2018). Ethical considerations when conducting joint interviews with close relatives or family: an integrative review. *Scandinavian Journal of Caring Sciences, 32*(2), 515-526. https://doi.org/10.1111/scs.12535

Korstjens, I., & Moser, A. (2017). Series: Practical guidance to qualitative research. Part 2: Context, research questions and designs. *European Journal of General Practice, 23*(1), 274-279. https://doi.org/10.1080/13814788.2017.1375090

Korstjens, I., & Moser, A. (2018). Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis. *The European Journal Of General Practice, 24*(1), 9-18. https://doi.org/10.1080/13814788.2017.1375091

Krauss, S. E., & Peredaryenko, M. S. (2013). Calibrating the human instrument: Understanding the interviewing experience of novice qualitative researchers. *Qualitative Report, 18*(43), 1-17. https://search-ebscohost-

com.ezp.waldenulibrary.org/login.aspx?direct=true&db=a9h&AN=91747682&site=eds-live&scope=site

Kulkarni, G. (2019). Transitioning an enterprise from COBIT 5 to COBIT 2019. *COBIT Focus*, 1-9. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=bth&AN=139604912&site=eds-live&scope=site

Kuzmenko, I., Orlovskyi, R., Petrenko, P., Pochtovyi, M., & Vakulyk, O. (2020). Cybersecurity as a component of the national security of the state. *Journal of Security & Sustainability Issues, 9*(3), 775-784. https://doi.org/10.9770/jssi.2020.9.3(4)

Kwon, Y. J., Lee, S.-Y. T., & Yang, A. (2020). The impact of information sharing legislation on cybersecurity industry. *Industrial Management & Data Systems, 120*(9), 1777-1794. https://doi.org/10.1108/IMDS-10-2019-0536

Kwong, Y. K., McQuaid, P., & Pettit, A. (2016). Independent quality and risk assessment in major IT projects of large enterprises. *Software Quality Professional, 19*(1), 9-22. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=edb&AN=120476248&site=eds-live&scope=site

Lee, J. (2017). Strategic risk analysis for information technology outsourcing in hospitals. *Information & Management, 54*(8), 1049-1058. https://doi.org/10.1016/j.im.2017.02.010

Leedy, P. D., & Ormrod, J. E. (2016). *Practical research: Planning and design* (12th ed.). Pearson.

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine & Primary Care, 4*(3), 324-327. https://doi.org/10.4103/2249-4863.161306

Liu, L. (2018). *Heart failure: Epidemiology and research methods.* Elsevier B.V. https://doi.org/10.1016/B978-0-323-48558-6.00005-0

Liu, X., Zhang, J., & Zhu, P. (2016). Dependence analysis based cyber-physical security assessment for critical infrastructure networks. *IEEE Proceedings: 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) Information Technology, Electronics and Mobile Communication Conference (IEMCON).* Vancouver: IEEE. https://doi.org/10.1109/IEMCON.2016.7746296

Lo, M. C., Peikari, H. R., Shah, M. H., & Ramayah. (2018). Patients' perception of the information security management in health centers: The role of organizational and human factors. *BMC Medical Informatics & Decision Making, 18*(1), 1-13.

Lü, J., Wang, P., Xu, S., & Zhang, C.-X. (2019). Spectral learning algorithm reveals propagation capability of complex networks. *IEEE Transactions on Cybernetics, 49*(12), 4253-4261. https://doi.org/10.1109/TCYB.2018.2861568

Lub, V. (2015). Validity in qualitative evaluation: Linking purposes, paradigms, and perspectives. *International Journal of Qualitative Methods, 14*(5), 1-8. https://doi.org/10.1177/1609406915621406

Lusinchi, D. (2017). The rhetorical use of random sampling: Crafting and communicating the public image of polls as a science (1935–1948). *Journal of the History of the Behavioral Sciences, 53*(2), 113-132. https://doi.org/10.1002/jhbs.21836

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

Markelj, B., & Vrhovec, S. (2018). Relating mobile device use and adherence to information security policy with data breach consequences in hospitals. *Journal of Universal Computer Science, 25*(5), 634-645. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=edswsc&AN=000438471200006&site=eds-live&scope=site

Marquez, J. (2017). Setting the record straight: Convincing management of COBIT's value in risk management. *COBIT Focus*, 1-3. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=bth&AN=120638431&site=eds-live&scope=site

Marting, R. (2018). HIPAA: Answers to your frequently asked questions. *Family Practice Management, 25*(2), 12-16. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=mnh&AN=29537247&site=eds-live&scope=site

Mattioli, M. (2018). Security incidents targeting your medical practice. *MD Advisor: A Journal For New Jersey Medical Community, 11*(2), 4-10.

http://search.ebscohost.com/login.aspx?direct=true&AuthType=shib&db=mdc&AN=30570893&site=eds-live&scope=site

Maxwell, J. A. (2015). Expanding the history and range of mixed methods research. *Journal of Mixed Methods Research, 10*(1), 12-27. https://doi.org/10.1177/1558689815571132

Mayer, I. (2015). Qualitative research with a focus on qualitative data analysis. *International Journal of Sales, Retailing & Marketing, 4*(9), 53-67. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=bth&AN=116381445&site=eds-live&scope=site

McEvilley, M., Oren, J. C., & Ross, R. (2016). Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems. *NIST Special Publication, 800-160*, 1-261. https://doi.org/10.6028/NIST.SP.800-160

Moeini, M., & Rivard, S. (2019). Responding-or not-to information technology project risks: An integrative model. *MIS Quarterly, 43*(2), 475-500. https://doi.org/10.25300/MISQ/2019/14505

Monken, J., Sand, A. F., & Trimble, D. (2017). A framework for cybersecurity assessments of critical port infrastructure. *IEEE Proceedings: 2017 International Conference on Cyber Conflict (CyCon U.S.).* Washington, DC: IEEE. https://doi.org/10.1109/CYCONUS.2017.8167506

Murashbekov, O. (2019). Challenges on introducing information security standards: A case study. *Journal of Security & Sustainability Issues, 8*(4), 665-674. https://doi.org/10.9770/jssi.2019.8.4(10)

Nan, F., Wandong, C., & Ye, Y. (2016). Network & information system security risk assessment technology. *IEEE Proceedings: 2016 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, 397-401. https://doi.org/10.1109/IBCAST.2016.7429909

Nassaji, H. (2015). Qualitative and descriptive research: Data type versus data analysis. *Language Teaching Research, 19*(2), 129-132. https://doi.org/10.1177/1362168815572747

Nikishova, A., & Vitenburg, E. (2019). Project of automated system's information security system selection. *IEEE Proceedings: 2019 International Science and Technology Conference "EastConf"*. Vladivostok: IEEE. https://doi.org/10.1109/EastConf.2019.8725345

National Institute of Standards and Technology. (2004). Standards for security categorization of federal information and information systems. *Federal Information Processing Standards Publication, 199*, 1-13. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

National Institute of Standards and Technology. (2010). *Guide for applying the Risk Management Framework to federal information systems: A security life cycle approach* (1 ed.). Gaithersburg, Maryland, USA: National Institute of Standards and Technology. https://doi.org/10.6028

National Institue of Standards and Technology. (2013). Security and privacy controls for federal information systems and organizations. *NIST Special Publication, 800-53*, 1-462. https://doi.org/10.6028/NIST.SP.800-53r4

National Institue of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity.* National Institute of Standards and Technology. https://www.nist.gov/cyberframework/framework

National Institue of Standards and Technology Joint Task Force. (2018). Risk management framework for information systems and organizations (NIST Special Publicaiton 800-37). *NIST Journal of Research*. https://doi.org/10.6028/NIST.SP.800-37r2

National Research Act of 1974, Pub. L. 93-348, 88 Stat. 342 (1974). Office of the National Coordinator for Health Information Technology. (2019). *What is an electronic health record (EHR)?* https://www.healthit.gov/faq/what-electronic-health-record-ehr

Patton, M. Q. (2015). *Qualitative research and evaluation methods: Integrating theory and practice* (4th ed.). Sage Publications.

Polkinghorne, D. E. (2006). Narrative configurative in qualitative analysis. *International Journal of Qualitative Studies in Education, 8*(1), 5-232. https://doi.org/10.1080/0951839950080103

Porcher, R., Ravaud, P., Tran, V.-C., & Tran, V.-T. (2017). Predicting data saturation in qualitative surveys with mathematical models from ecological research. *Journal of Clinical Epidemiology*, 82:71-78. https://doi.org/10.1016/j.jclinepi.2016.10.001

Rashidi, A. J., & Shakibazad, M. (2020). New method for assets sensitivity calculation and technical risks assessment in the information systems. *IET Information Security, 14*(1), 133–145. https://doi.org/10.1049/iet-ifs.2018.5390

Retnowardhani, A., & Yoseviano, H. F. (2018). The use of ISO/IEC 27001: 2009 to analyze the risk and security of information system assets: Case study in XYZ, LTD. *IEEE Proceedings: 2018 International Conference on Information Management and Technology (ICIMTech)* (pp. 21–26). Jakarta: IEEE. https://doi.org/10.1109/ICIMTech.2018.8528096

Rezaeibagha, F., Susilo, W., & Win, K. T. (2015). A systematic literature review on security and privacy of electronic health record systems: Technical perspectives. *Health Information Management Journal, 44*(3), 23-38. https://doi.org/10.1177/183335831504400304

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *Journal of Psychology, 91*(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

Rotella, P. (2018). Software security vulnerabilities: Baselining and benchmarking. *IEEE Proceedings: 2018 IEEE/ACM 1st International Workshop on Security Awareness from Design to Deployment (SEAD)* (pp. 3-10). Gothenburg: IEEE. https://doi.org/10.23919/SEAD.2018.8472847

Rowley, J. (2002). Using case studies in research. *Management Research News, 25*(1), 16-27. https://doi.org/10.1108/01409170210782990

Sadoughi, F., & Zarei, J. (2016). Information security risk management for computerized health information systems in hospitals: A case study of Iran. *Risk Management and Healthcare Policy, 2016*(1), 75-85. https://ezp.waldenulibrary.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=edsdoj&AN=edsdoj.55146d57f1ba4f18943816972c86e5ad&site=eds-live&scope=site

Siedlecki, S. L. (2020). Understanding descriptive research designs and methods. *Clinical Nurse Specialist: The Journal for Advanced Nursing Practice, 34*(1), 8-12. https://doi.org/10.1097/NUR.0000000000000493

Small, A., & Wainwright, D. (2018). Privacy and security of electronic patient records: Tailoring multimethodology to explore the socio-political problems associated with Role Based Access Control systems. *European Journal of Operational Research, 265*(1), 344-360. https://doi.org/10.1016/j.ejor.2017.07.041

Snelgrove, S., & Vaismoradi, M. (2019). Theme in qualitative content analysis and thematic analysis. *Forum: Qualitative Social Research, 20*(3), 1-14. https://doi.org/10.17169/fqs-20.3.3376

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

Strawn, G. O., & Vagoun, T. (2015). Implementing the federal cybersecurity R&D strategy. *Computer (New York), 48*(4), 45-55. https://doi.org/10.1109/MC.2015.111

Surmiak, A. (2018). Confidentiality in qualitative research involving vulnerable participants: Researchers' perspectives. *Forum Qualitative Sozialforschung, 19*(3), 393-418. https://doi.org/10.17169/fqs-19.3.3099

Sween-Cadieux, E. M., & Turcotte-Trembley, A.-M. (2018). A reflection on the challenge of protecting confidentiality of participants while disseminating research results locally. *BMC Medical Ethics, 19*(Suppl 1), 45. https://doi.org/10.1186/s12910-018-0279-0

Thomas, M. (2018). A new COBIT is in town and I really like how it looks. *COBIT Focus*, 1-8. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=bth&AN=133592800&site=eds-live&scope=site

Thompson, J. M., & Zandona, D. J. (2017). Going beyond compliance: A strategic framework for promoting information security in hospitals. *Health Care Manager, 36*(4), 364-371. https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=edo&AN=126065302&site=eds-live&scope=site

Tian, J., Xiao, L., & Yang, Y. (2016). Transmission of clinical information based on HL7 CDA standard. *IEEE Proceedings: 2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS)* (pp. 949-952). Beijing: IEEE. https://doi.org/10.1109/ICSESS.2016.7883222

U.S. Department of the Interior. (2019). *DOI security assessment & authorization*. Retrieved December 2019, from U.S. Department of the Interior - Office of Chief Information Officer: https://www.doi.gov/ocio/customers/assessment

Vanderpool, D. (2019). HIPAA Compliance: A common sense approach. *Innovations in Clinical Neuroscience, 16*(1/2), 38-41. https://eds-b-ebscohost-com.ezp.waldenulibrary.org/eds/pdfviewer/pdfviewer?vid=0&sid=0cd1fb17-1942-4d16-ae34-bf98f3a0c4a5%40sessionmgr101

Vinnakota, T. (2016). A second order cybernetic model for governance of cyber security in enterprises. *IEEE Proceedings: 2016 IEEE 6th International Conference on Advanced Computing (IACC)* (pp. 706-710). Bhimavaram: IEEE. https://doi.org/10.1109/IACC.2016.136

Walford, G. (2018). The impossibility of anonymity in ethnographic research. *Qualitative Research, 18*(5), 516-525. https://doi.org/10.1177/1468794118778606

Appendix A: Collaborative Institutional Training Initiative Researchers Certificate

Student Researchers Basic Course Certificate

CITI PROGRAM

Completion Date 08-Dec-2019
Expiration Date N/A
Record ID 29579045

This is to certify that:

Ian Wilkinson

Has completed the following CITI Program course:

Student Researchers (Curriculum Group)
Student Researchers (Course Learner Group)
1 - Basic Course (Stage)

Under requirements set by:

Walden University

CITI
Collaborative Institutional Training Initiative

Verify at www.citiprogram.org/verify/?wece14b90-a7b8-4371-adf6-0527565e1cdc-29579045

Appendix B: Interview Questions

1. What experiences have you had implementing strategies toward the IT security and administration of government health organizations?

2. What were some of the technologies you've used and your perceptions of those technologies to secure PHI?

3. How do you identify threats to protected health data, and how are those threats mitigated?

4. What procedures and mechanisms have you used to decrease vulnerabilities and ensure health information security software and technologies have the latest software patches or firmware?

5. What procedures are in place to notify users or shareholders of potential or realized breaches of data?

6. What policies and procedures are in place to ensure compliance with state, government, and organizational laws, policies, guidelines, and regulations regarding PHI?

7. How are the information systems of the organization categorized to support adequate selection and implementation of security controls?

8. How are the security controls assessed and monitored after implementation, and what are the processes in place to support periodic assessments to sustain the security posture of the organization?

9. What are the procedures for authorizing an information system, and what position or organizational level is responsible for authorizing information security systems on the network?

10. Is there anything else that you would like to include concerning risk-based strategies for cybersecurity that was not covered?

Appendix C: Case Study Data Collection Protocol

1) Data Collection Protocol Purpose
   a) The protocol is to be used as a guide from the planning phases to the execution of the research to direct the data collection processes and techniques used by the researcher.
   b) The use of the data collection protocol also assists in ensuring the reliability and organization of the research conducted by the researcher.

2) Data Collection Procedures
   a) Data will be collected from the following sources:
      i) Participant Interviews (semi-structured)
      ii) Observations
      iii) Field Notes
      iv) Historical/ Organizational Documentation (policies, SOPs, reports, standards, guides, etc.)
   b) Participants will consist of 1-2 interviewees from each of the four health organizations chosen in the mid-west of the United States that have successfully implemented or subscribe to a risk management strategy
   c) Participants and organizations will be identified pending a positive response to the invitation letter and selected pending a positive receipt of the participant signed informed consent form

3) Data Collection Tools
   a) Field Notes
   b) Audio Recordings

4) Interview Questions
   1.