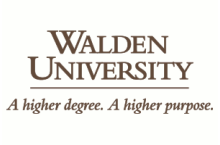

2020

Technical Strategies Database Managers use to Protect Systems from Security Breaches

Leonard Ogbonna
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Leonard Ogbonna

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

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

Walden University
2020

Abstract

Technical Strategies Database Managers use to Protect Systems from Security Breaches

by

Leonard Ogbonna

MS, Long Island University, 2004

MA, Fordham University, 1999

BD, Bigard Memorial Seminary, 1993

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

March 2020

Abstract

Healthcare organizations generate massive amounts of data through their databases that may be vulnerable to data breaches due to extensive user privileges, unpatched databases, standardized query language injections, weak passwords/usernames, and system weaknesses. The purpose of this qualitative multiple case study was to explore technical strategies database managers in Southeast/North Texas used to protect database systems from data breaches. The target population consisted of database managers from 2 healthcare organizations in this region. The integrated system theory of information security management was the conceptual framework. The data collection process included semistructured interviews with 9 database managers, including a review of 14 organizational documents. Data were put into NVivo 12 software for thematic coding. Coding from interviews and member checking was triangulated with corporate documents to produce 5 significant themes and 1 subtheme: focus on verifying the identity of users, develop and enforce security policies, implement efficient encryption, monitor threats posed by insiders, focus on safeguards against external threats, and a subtheme derived from vulnerabilities caused by weak passwords. The findings from the study showed that the implementation of security strategies improved organizations' abilities to protect data from security incidents. Thus, the results may be applied to create social change, decreasing the theft of confidential data, and providing knowledge as a resource to accelerate the adoption of technical approaches to protect database systems rom security incidents.

Technical Strategies Database Managers use to Protect Systems from Security Breaches

by

Leonard Ogbonna

MS, Long Island University, 2004

MA, Fordham University, 1999

BD, Bigard Memorial Seminary, 1993

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

March 2020

Dedication

I dedicate this work to my late parents, Maria and Modestus Ogbonna. Though you have passed from this life, your memories are alive. I will always treasure your ineffable faith and dedication. I hold these sterling qualities and genteel mannerisms close to my heart.

Acknowledgments

First all, I am thankful to God for the gift of life and health. I dedicate the successful completion of this study to my entire doctoral committee. To my exceptional mentor and doctoral chair, Dr. Steven Case, for spending several hours of your time, encouraging, advising, and guiding me through the doctoral study, I owe you my enduring gratitude. Without your meticulous feedback, I wouldn't have completed the program. To my second committee member Dr. Gail Miles, I am grateful for your guidance through the process for your suggestions, thoughts, and feedback as the study developed. To my URR, Dr. Gary Griffith, I am grateful for your support throughout the process. I appreciate your feedback and recommendations. To the rest of the DIT staff and Walden University, I am thankful. Lastly, I am so grateful to my whole family, to my stepmother Lady (Mrs.) Eunice, my elder brother Francis, and the rest of my family for your encouragement and inspiration during the preparation of this dissertation. To all my friends, I am indeed thankful for your support.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

Databases hold one of the most valuable assets of organizational information systems. For instance, healthcare organizations depend on databases to store, access and retrieve patient information as well as meet organizational goals and business objectives. Without the deployment of security strategies, databases could be exposed to system flaws. Databases are vulnerable to data breaches due to systems weaknesses (Ahmad, Saad, & Mohaisen, 2019). System faults can result from standardized query language injection, misconfigured databases, inadequate auditing, including, unpatched databases, and deployment failures.

Data breaches across the globe have forced database managers to implement various security approaches to secure organizational database systems. Database managers rely on these methods for day-to-day businesses. High-profile data breaches across different healthcare organizations might signify failures in implementing appropriate security strategies used to address systems' weaknesses. Security strategies can involve executing sophisticated passwords, awareness of internal and external threats, and prioritizing vulnerability remediation. Determining technical approaches needed to safeguard healthcare organizational database systems may lead to adequate system protection and minimize data breaches as a result of system vulnerabilities. It is important to address growing data vulnerabilities through the analysis of technological and human threats (Ruohonen, Rauti, Hyrynsalmi, & Leppänen, 2018). Thus, database managers must implement different security strategies to address not only the recurrent weaknesses within the database system but equally human and technical risks.

Background of the Problem

Security breaches have become an everyday routine for many healthcare organizations. Almost every month, there may be an announcement of a data breach. For example, the number of attacks exploiting system weaknesses increased to 142 million in 2014 from 83 million in 2013 and 34 million in 2012 (Murtaza, Khreich, Hamou-Lhadi, & Bener, 2016). Major data breaches, like Sony's, or breaches in which massive amounts of sensitive personal information were exposed, like the 2015 Anthem breach, have attracted media attention. In 2014, 904 million records got exposed within the first 9 months, 95% increase from the same period in 2013 (Ashenmacher, 2016). The attack compromised a range of personal information.

Regardless of technical strategies and defensive measures employed to protect organizational database systems by different organizations, data breach incidents continue to make headlines. Lawmakers have taken several actions to prevent data breaches, such as the passage of breach notification laws, increased spending to fund security initiatives, reporting requirements, and mandated data privacy requirements (Sen & Borle, 2015). However, data breaches are still on the rise. In response to the growing number of never-ending privacy violations, database managers must strive to develop and implement effective countermeasures to address such problems. Consequently, database managers must develop effective technical strategies to manage cyber threats orchestrated by cybercriminals and insiders, including safeguarding personal information against data breach threats.

Problem Statement

Cyber attackers have used multiple vulnerabilities to penetrate databases resulting in data breaches (Vu, Khaw, & Tsong Yueh, 2015). Accidental loss resulting from device theft represented approximately 94% of healthcare data breaches (Luna, Rhine, Myhra, Sullivan, & Kruse, 2016), and roughly 47% of breaches are characterized as theft and hacking (Srivastava & Kumar, 2015). The general information technology (IT) problem is that many healthcare organizations experience data breaches due to vulnerabilities in database systems. The specific IT problem is that some database managers in Southeast/North Texas lack technical strategies used to protect database systems from data breaches.

Purpose Statement

The purpose of this qualitative multiple case study was to explore technical strategies database managers in Southeast/North Texas used to protect database systems from data breaches. The targeted population consisted of database managers from two healthcare organizations in Southeast/North Texas who have technical strategies used to protect database systems from data breaches. The implications of positive social change include the potential for decreasing the theft of confidential or sensitive data. Implementing data breach strategies in healthcare institutions may help hospital leaders minimize the breach or loss of personally identifiable information.

Nature of the Study

Different research methods, such as qualitative, quantitative, and mixed methods were evaluated for the study. I chose the qualitative approach for the research, which is

used to classify the perception of research participants (Posey, Roberts, Lowry, & Hightower, 2014). This method was chosen because the intent was to explore the perception of database managers. Conversely, the quantitative approach is employed to test a hypothesis about relationships or differences between variables (Scrutton & Beames, 2015). Mixed methods research involves the combination of quantitative and qualitative approaches within a single research study (Thiele, Pope, Singleton, & Stanistreet, 2018). Because I did not test a hypothesis, neither quantitative nor mixed methods were applicable.

I selected a multiple case study design to investigate the technical strategies database managers used to protect systems from security breaches. Such helped to answer *what* and *how* questions and allowed me to interact with participants to understand their experiences. The method is designed to capture the richness, diversity, and intensity of a given phenomenon from multiple viewpoints (Civitillo, Juang, Badra, & Schachner, 2019). I used a multiple case study design to collect and analyze various cases.

Other designs were considered but not chosen. The phenomenological method is used to understand the feelings and lived experiences of individuals who have experienced a phenomenon (VanScoy & Evenstad, 2015). However, the objective of the study was not to understand the lived experiences of individuals who have experienced a phenomenon but to explore technical strategies participants used to protect database systems. Additionally, ethnography involves understanding the cultural behaviors of participants (Baskerville & Myers, 2015), but the study was not used to gain knowledge about the cultural patterns of participants. Finally, narrative research constructs a story

about an individual's experience. The model articulates the story of individuals, including requesting one or more persons to provide stories about their lives (Van der Vyver & Marais, 2015). The narrative design was unsuitable, as the intent was not about providing stories about people's lives but to explore the technical strategies database managers used to protect database systems from data breaches.

Research Question

What technical strategies do database managers in Southeast/North Texas use to protect database systems from data breaches?

Interview Questions

1. What security strategies could be utilized to combat database threats posed by hackers?
2. How can external and insider threats compromise your organizational database system
3. What challenges do you have in addressing the security threats posed by cybercriminals or social engineers?
4. What technical strategies have you employed to protect database systems from data breaches?
5. What programs do you use to protect database systems from security vulnerabilities?
6. What measures do you take to mitigate risk in case of database compromise?
7. How does your experience in failures of technical and non-technical controls contribute to security breaches?

8. What additional information can you provide to assist me in understanding the phenomenon?

Conceptual Framework

I used the integrated system theory of information security management as the conceptual framework. Hong, Chi, Chao, and Tang (2003) developed the integrated system theory of information security management, incorporating prior theories relating to different perspectives from the security policy, risk management, control and auditing, management systems, and contingency theories to build the integrated system theory. Hong et al. used their approach to provide a rich information security strategy, procedures, and methods for researchers, information security decision-makers, planners, providers, and users to get a better understanding of information security regarding different perspectives.

Other researchers have demonstrated the use of the integrated systems theory. For example, Young and Leveson (2014) employed the theory to assess the system engineering approach to security and safety, including the use of schemes in resolving conflicts between safety and security in the development processes. The integrated system theory of information security management is an inclusive framework that can be used as a guide to empirical studies and a managerial measure to elevate an organization's security level (Hong, Yen-Ping Chi, Chao, & Tang, 2006). The integrated system method of information security management was chosen as an appropriate conceptual framework to guide the selected study. The technique might be helpful in understanding data privacy breaches, record exposure, and theft of confidential data. The

theory can also be a building block for further information security management and maybe a guide for future empirical studies. The main concepts from the theory include (a) security policy, (b) risk management, (c) internal control and auditing, (d) management, and (e) contingency theory. These concepts guided the research as I sought to understand data breach strategies database managers used to protect database systems from data breaches.

Definition of Terms

Throughout the study, I used the following terms. Defining them are essential for more precise understanding and clarification.

Breach: A breach is unauthorized access or compromise of personal information such as names, dates of birth, or social security number (Hemphill & Longstreet, 2016).

Computer virus: A self-replicating program on the network that uses a system to send copies of itself to other computers within the network (Zhu & Cen, 2017).

Cyberattack: A complex and sophisticated attack involving the exploitation of critical infrastructure assets, which could cause significant damage to systems (Genge, Kiss, & Haller, 2015).

Cybercrime: Cybercrime refers to criminal acts committed by using electronic communication networks and information systems against targeted networks with the intent to steal confidential data or destroy network systems (Bergmann, Dreißigacker, von Skarczinski, & Wollinger, 2018).

Database: A collection of data in the form of schemas, tables, queries, reports, or other objects. Technically, anything that stores data for later retrieval is a database (Richardson, 2015).

Data breach: Involves unauthorized access to sensitive or confidential data which might result in the compromise of confidentiality, integrity, or the availability of data (Sen & Borle, 2015).

Database manager: Those who design, develop, and address challenges facing database systems, such as cyber threats, denial of service attacks, or privacy concerns (van Dijk, Kalidien, & Choenni, 2018).

Data vulnerability: A weakness within a systems' infrastructure which can diminish systems assurance, making such systems prone to cyber-attacks (Fonseca, Seixas, Vieira, & Madeira, 2014).

Insider threat: An insider threat occurs when a person authorized to perform specific actions within the organizational computer system abuse such privileges to harm systems network infrastructure (Tyler, 2016).

Security strategy: Refers to protective processes used to prevent unauthorized access to database infrastructure (Tan & Yu, 2018). These strategies include software/hardware measures such as password and firewall, antivirus protection, regular updates, system monitoring, or education of organizational employees.

Assumptions, Limitations, and Delimitations

Individuals view the world from different perspectives. To pursue objectivity, investigators must pay specific attention to their assumptions. Assumptions are subjective

perceptions of the researcher that might influence the investigator's viewpoints (Twining, Heller, Nussbaum, & Tsai, 2017). Limitations refer to boundaries or circumstances that might limit the researcher from achieving objective reality in a study (Hemkens, Contopoulos-Ioannidis, & Ioannidis, 2016). Delimitations refer to purposeful restrictions a researcher might impose on the research (Brusse, Kach, & Wagner, 2016).

Assumptions

Qualitative investigation begins with assumptions. Researchers should be mindful of their thoughts or beliefs and admit underlying assumptions in the pursuit of objectivity (Barnham, 2015). Assumptions may be used to indicate whether restrictive causes might affect the result of the study. I made several assumptions during the research. The first assumption is that some leaders of healthcare organizations concerned with data breach may be reluctant to participate in the study. The second assumption is that participants would respond truthfully and honestly to interviews and that data collection may not be exact or broad. The third assumption is that no form of bias either from participants or researcher would affect the research. The fourth assumption is that enough participants may not have been available for the study. The fifth assumption is that Southeast/North Texas would be an excellent place to recruit participants. The final assumption is that the face-to-face interview-questioning process would not affect the outcome of the investigation.

Limitations

Limitations are restrictive circumstances that might prevent the investigator from achieving objective goals. Reporting limitations of a study provide other researchers with

information when considering or planning to conduct similar research, as it helps indicate possible challenges in interpreting results (Hemkens et al., 2016). Some limitations for this study included (a) data collection could have been limited depending on the availability of participants, (b) the dataset may not contain all of the information relating to data breaches among organizations under study, (c) the study may not address all security strategies or the impact data breaches might have on healthcare systems, and (d) the results of the study are limited to healthcare organizations in Southeast/North Texas.

Delimitations

Delimitations describe the boundaries a researcher might set for the investigation. Delimitations are predetermined constraints that can be explained by the boundary limits (Brusse, Kach, & Wagner, 2016). The first delimitation is that the study was limited to database managers who are at least 21 years of age and have had at least 3 years of database managerial experience within the designated organizations. The second delimitation is that the investigation was limited to participants who meet specific criteria of eligibility. The third delimitation was the constraint of the sample size to two healthcare organizations. The last delimitation was the geographical area of the study, which was limited to Southeast/North Texas.

Significance of the Study

Contribution to IT Practice

The findings from the study include new insights regarding technical strategies database managers use to protect database systems from security breaches. Database managers face challenges between system flaws and security failures. Cybercriminals

take advantage of such failures to breach network infrastructure (Wagner, 2016). However, available research has not addressed critical issues in data security, such as technical insiders or database managers who manage organizational database infrastructures. Data breaches could arise when database professionals fail to respond to growing security threats (Manworren, Letwat, & Daily, 2016). Database managers need to focus on insiders in making the right decision when it comes to information security and how human behavior could generate serious data breaches (Li, Meng, Kwok, & Ip, 2017).

The study may provide healthcare organizations in Southeast/North Texas with an understanding of the factors that contribute to data breaches. The research is necessary because it might provide different strategies for data protection, such as enforcing restrictions on database access, ensuring operating systems are up to date, including applying security measures. It might create an information system that could span geographical boundaries, incorporate different cultures, and create awareness for ethical behaviors in using IT, especially concerning data privacy. Consequently, it may help leaders and policymakers understand the importance of IT, particularly regarding social and economic impact IT brings to developing nations, especially in providing culturally relevant programs that can enhance data security in IT. The implications of positive social change include the potential for decreasing the theft of sensitive protected data. Implementing data breach strategies in healthcare organizations may help minimize the breach or loss of personally identifiable information. It may serve as a tool for providing knowledge as a resource for hospital leaders to accelerate the adoption of technical

measures to protect their systems from data breaches. The study might help in establishing genuineness or originality of a subject in verifying information sources. Additionally, it might contribute to a responsible practice in checking that network devices perform as expected.

Implications for Social Change

This may impact social change because database managers and data owners are apprehensive of database systems due to system vulnerabilities, which may lead to security breaches. The research could provide information on IT security strategies to advance business objectives, benefitting database managers, and healthcare organizations. For example, healthcare organizations could use different security approaches to minimize database weaknesses by an understanding of the factors that contribute to data breaches.

Additionally, the benefits of data security are evident when database flaws are minimized, and the activities of cybercriminals regarding diminishing system assurance are contained. These benefits could reduce unauthorized access due to inadequate security strategies. Security strategies may help in decreasing the theft of sensitive protected data and serve as a tool for providing knowledge as a resource for hospital leaders to accelerate the adoption of technical measures to protect their systems from data breaches. It might create an information system that can span geographical boundaries, incorporate different cultures, and create awareness for ethical behaviors in using IT, especially concerning data privacy.

A Review of the Professional and Academic Literature

The purpose of this qualitative multiple case study was to explore technical strategies database managers used in protecting healthcare organizations from data breaches in Southeast/North Texas. I anchored the review of literature on the integrated system theory of the information security management model, which was the conceptual framework for studying the strategies database managers used to prevent data breaches in healthcare organizations. I organized the contents of the literature review with security strategies in mind and outlined the conceptual model by explaining the integrated systems theory of information security management. The literature review is organized by an examination of the conceptual framework, the development of the theory, supportive theories, contrasting theories, technical strategies, different types of data breaches, and the role of database managers.

A review of current literature provided a basis for the study based on gaps in the literature, especially for database managers in predicting organizational attitudes and behaviors toward information security management. Critical points found in the literature regarding the activities of insiders are related. Significant ideas relate to mechanisms such as authentication, intrusion detection systems (IDSs), or Encryption (You, Ogiela, Woungang, & Yim, 2016). Other crucial areas related to programs, education, and organizational policies as a way of curbing the activities of insiders (Lu, Sun, Liu, & Li, 2018). The behavior of organizational insiders has been explored but is under-explored by researchers. Many scholars have limited engagement in this area, and not much

research has been conducted on how to predict insider behavior in the use of healthcare database infrastructure.

A critical analysis of the literature review also guided the investigation in creating the foundation for the study, including establishing justification for technical strategies used to protect database systems from data breaches. The analysis of literature consisted of contemporary peer-reviewed journals from investigations related to data breaches gathered through a detailed search of online libraries, including the Walden Library, ProQuest database, EBSCO database, Sage Journals, dissertations, Google Scholar, Science Direct, including local and public libraries. The literature included a careful investigation of seminal and empirical articles related to data breaches. Search terms include *data breach, privacy breaches, database, database managers, database vulnerability, insider breaches, data availability, and technology threat avoidance theory, external breaches, cybercrime, social engineering, hacking, keylogging, and data confidentiality, denial of service, data integrity, deterrence theory,* and *cybersecurity*.

The review was aimed to find relevant journals and academic reports, seminal books, empirical, and current research in the area of study. During the search, I reviewed 330 articles for relevance. Out of that number, 272 sources were used for the literature review; 257 (89.7 %) were peer-reviewed articles and verified through Ulrich, and 176 (77.5.0%) of the references were used for the literature review. A total of 253 (91.1%) references were published within five years of completion of study (2015 through 2019), 2 (0.7%) were government sources, 4 (0. 8%) were books, and 1 (0.09%) were

dissertation. Two hundred and twenty-two (70.8%) of 253 peer-reviewed articles have an object identifier (DOI) assigned.

Integrated System Theory of Information Security Management

Hong et al. (2003) developed the integrated system theory of information security management in reaction to the security threats posed by cyber attackers and unauthorized users. The theory has five components: (a) security policy, (b) risk management, (c) internal control, (d) information auditing, and (e) contingency management. An in-depth information security plan may require a combination of security measures such as authentication, IDSs, malware programs, or employee training to confront security threats. Organizations might utilize comprehensive information security management to generate security reports, including strategies to minimize security incidents (Steinbart, Raschke, Gal, William, & Dilla, 2016). Thus, the theory can be useful in explaining how a comprehensive security plan may help industries in understanding information security management strategies, including measures to minimize security threats.

Further, Hong et al. (2006) used a comprehensive information security policy focused on implementing different security mechanisms to underscore the essence of inclusive security measures. With the prevalence of e-commerce, information security is important to many organizations, so several industries have set up information security policies to safeguard network infrastructures from security threats (Hong et al., 2006). Organizational leaders believe that building an integrated security system may deter improper actions orchestrated by cybercriminals and increase the awareness of potential security threats and attacks. For example, without inclusive system security, healthcare

organizational security measures may not be able to withstand different security threats posed by criminals globally. Thus, comprehensive information security policies may contribute to better security measures in protecting organizational system infrastructures.

Different facets of the integrated system approach relate to hardware, administrative processes, and software, including technological procedures employed by system administrators to regulate and protect information resources (Ismail, Sitnikova, & Slay, 2014). Through the combination of information security practices, system administrators can analyze systems' infrastructures to determine the most likely route cyber attackers may take to diminish system security (Ismail et al., 2014; Young, & Leveson, 2014). Integration of technological procedures and administrative processes may include risk assessment, security policies, education, and training, including system audit to ensure system performance meet security mechanisms needed to diminish belligerent activities initiated by cybercriminals. Although the integration of these components can be challenging, the benefits are significant in securing information resources.

Organizational leaders can utilize the theory to implement adequate security strategies to achieve business objectives. An effective security strategy may involve protecting confidentiality, integrity, and availability of data, including determining vulnerabilities that might exist within the system (Ismail et al., 2014). Organizational network systems face the possibilities of cyberattacks, and information security management plays an essential role in drawing the roadmap of information security (Yang, Ku, & Liu, 2016). By implementing security strategies such as educational

programs, policies, or training, database managers can solve security issues that may lead to data breaches. Thus, a combination of security strategies may help security leaders implement security measures to achieve business objectives.

Many researchers have used the theory to analyze information systems and security measures. May and Lending (2015) used the model to provide students and faculty with a holistic understanding of the information systems field. Using the concept for understanding the diversity of information systems approach, May and Lending demonstrated that an information system might relate to a combination of technical and socio-organizational subsystems. By combining information system security measures, organizational leaders may provide a complete understanding of systems security. A holistic understanding of information systems may focus on different security measures, including how such constituent parts may interrelate to protect systems from security breaches. Such steps are necessary for understanding comprehensive methods in security systems.

Young and Leveson (2014) also employed the theory to understand, assess, and scrutinize inadequate security measures, including safety issues among organizations. Through the integration of security measures, database managers can address poor security strategies at its earliest stages (Yang et al., 2016). An appropriate combination of security systems such as authentication, encryption, or IDSs could prevent unauthorized access, illegal use, disclosure, disruption, modification, or destruction of information. Inadequate security measures may be due to database managers engaging in the insufficient firewall, lack of adequate controls, inadequate password protection, reduced

patching practices, and poor employee training. Although organizations may experience challenges resulting from weak security measures, understanding and scrutinizing different security strategies may help corporations in resolving security issues (Soomro, Shah, & Ahmed, 2016).

Additionally, Abdullahi and Orukpe (2016) used theory to emphasize the importance of effective security systems in institutions of higher learning. The domain entails using a standard security plan that may comprise of access control system, IDS, burglar alarm system, including video surveillance (Abdullahi & Orukpe, 2016). Abdullahi and Orukpe found that securing a university campus can be achieved through the integration of different security measures. Furthermore, the integrated system should be supported by a set of management practices such as education, programs, or training since access control mechanisms, or IDS cannot protect security systems from actions that may result from human activities. Thus, an effective security system needs to be combined with management practices.

Though the theory has been useful in addressing security management, because of criticisms that the integrated systems theory of information security management approach was limited to computer or network infrastructure, researchers like You, Cho, and Lee (2016) expanded the method to cover infrastructures such as power plants or water utilities. With continuous data breaches, critical infrastructures, including security measures that monitor such infrastructures, may be at risk. These infrastructures face possible cyberattacks, and by integrating different security measures, corporate leaders might advance systems' control (Ismail et al., 2014). Critical infrastructures connected

over the network are vital to businesses and national security, and as such, a compromise of such systems by hackers could trigger a national disaster. Thus, expanding the integrated system theory to include critical infrastructures can address significant security breaches.

Contrasting theories. In addition to integrated system theory, researchers have used other methods and models, such as general deterrence theory and routine activity theory, to examine information security issues. General deterrence theory was developed in 1959 by Bernard Brodie to reduce the extent to which people engage in deviant behavior. Deterrence is said to occur when people avoid crimes because of the costs of an unpleasant consequence of those crimes (Bhattacherjee & Shrivastava, 2018). Deterrence theory suggests that the threat of sanctions can alter employee actions when the individual weighs a possible penalty against a potential benefit (Willison & Warkentin, 2013). For example, when healthcare employees utilize systems databases, they may modify their behavior if they believe that unethical use of the organizational database may be sanctioned. Although healthcare employees may want to act in unusual ways, the threat of sanction may force them to change their behavior.

Deterrence theory also helps explain that as a result of data breaches against industries, individuals who perceive that their deviant behavior may be detected will less likely violate organizational security policies (Lijiao, Wenli, Qingguo, & Smyth, 2014). However, employee violation of security policies might be non-volitional such as accidental entry of incorrect data that could threaten data integrity (Willison & Warkentin, 2013). Furthermore, employee actions might include behaviors that are not

motivated by malicious intentions. Although computer violations may be non-volitional activities, such actions could compromise organizational computer systems and might likely lead to data breaches. Thus, the fear of punishment could still deter individuals from engaging in behaviors that may violate organizational system policies.

Additionally, the deterrence theory illustrates how dissuasion methods might inhibit undesirable actions like criminal behavior due to the threat of punishment (Yoo, Sanders, Rhee, & Choe, 2014). For example, individuals may be dissuaded from committing criminal acts if they have expectations of being caught (Chen, Wu, Chen, & Teng, 2018; Lowry, Posey, Bennett, & Roberts, 2015). Deterrence measures are effective strategies in contending illegal system activities (Yoo et al., 2014). Although deterrence measures are necessary to fight criminal activities within the systems' network, mandatory punishment is also essential in the abuse of systems infrastructure (Lowry et al., 2015). If users realize the probability of getting caught is high, they could be dissuaded from illegal computer actions due to the threat of punishment, making dissuasion methods effective in dealing with potential illegal activity.

Another contrasting theory was the routine activity theory, developed in 1979 by Cohen and Felson. The theory emphasizes that the absence of a capable administrator leads motivated offenders to carry out incidents of crime on victims or targets. Furthermore, routine activity theory is focused on computer crimes committed by insiders or cybercriminals due to the absence of a competent or skilled system manager, as the absence of capable managers may give rise to illegal activities (Cohen & Felson, 1979). For example, in the absence of a capable manager, each completed system violation

could require an offender with both criminal inclination and the ability to carry out computer violation (Cohen & Felson, 1979; Leukfeldt & Yar, 2016). The ability to carry out computer offenses within a healthcare database, for example, may depend on the absence of a capable database manager. Routine activity theory also assumes that people make rational choices when they commit unauthorized system violations. Such actions may involve occasions where a cybercriminal may illegally hack a computer system, alter system infrastructure, store or retrieve data, including changing a database resource with the intent to create occasions that could lead to data breaches. Thus, system offenders could be motivated to launch a crime whenever a suitable target emerges in the absence of an experienced manager.

Researchers have supported the use of routine activity theory to examine issues such as insider threats to security (Pratt & Turanovic, 2016). The theory helps explain that violations of an insider attack could materialize if the conditions are right and targets are suitable (Jingguo, Gupta, & Rao, 2015). Because insiders engage in routine access within the systems infrastructure due to their job responsibilities, such systems could likely be violated (Leukfeldt & Yar, 2016). Insider violations may happen depending on insiders' knowledge of the information environment, the range of technical and managerial controls, including the understanding of system characteristics (Jingguo et al., 2015). Insiders could figure out when system conditions are suitable to launch an attack if capable guardians are absent and targets are suitable. Thus, insiders' security threats could pose a significant concern for industries.

Supportive theories. Researchers have also employed the technology threat avoidance theory to evaluate how systems exposure could trigger malicious threats. Liang and Xue developed the theory to demonstrate how computer users may react when they perceive a threat to systems infrastructure. The model involves a combination of different disciplines, including risk analysis, information systems, healthcare, and psychology (Liang & Xue, 2009). Similar to general deterrence theory, investigators have used the concept to include employee negligence to organizational security policies, including computing behaviors such as inappropriate use of computers, network resources, passwords, and email (Chen, X., Wu, Chen, L., & Teng, 2018). These employee behaviors can be detrimental to organizational information systems. For instance, malicious threats could result if database managers do not implement anti-virus systems, vulnerability scanners, firewalls, or IDSs that could protect systems infrastructure from data breaches.

However, according to the theory, organizations may avoid malicious threats through safeguarding measures. Liang and Xue (2009) identified several steps such as usernames, passwords, or intrusive defensive mechanisms. Safeguarding measures relate to circumstances in which organizational leaders may provide programs such as anti-phishing education (Liang & Xue, 2009). Employing safeguarding measures could help in averting system threats and may prevent phishing schemes aimed at stealing confidential information such as passwords or other identifying data from victims (Liang & Xue, 2009). However, safeguarding measures alone may not protect corporations from all forms of malicious attacks since such measures need to be complemented with

employee behavior (Ikhalia, Serrano, Bell, & Arreymbi, 2017). Thus, a combination of safeguarding procedures could protect corporations from malicious threats.

According to Vance, Lowry, and Eggett (2015), organizations may adjust the behavior of insiders to the level of security risk. Vance et al. (2015) argued that behavioral concerns against system infrastructure might force organizational leaders to provide employees with education, programs, or training. Scholars in system security recognize that an organization's information security depends on insiders who have access to organizational data systems (Vance et al., 2015). Furthermore, Burns, Posey, Roberts, and Lowry (2017) debated that threats posed by insiders, or authorized organizational contractors may address how human behavioral actions may impact system availability, confidentiality, and integrity. While some corporate leaders may neglect insider behavior, such disregard of insider behavioral concerns may put organizational systems infrastructure at risk.

System flaws have been identified to generate security breaches. Padayachee (2016) claimed that organizations might minimize data breaches by focusing on system flaws and weaknesses that have to be present for a system to be compromised. Such occasions could relate to system vulnerabilities or employee behavioral actions, which could lead to system compromise (Warkentin, Johnston, Shropshire, & Barnett, 2016). Warkentin et al. argued that employee behavioral actions such as the opening of emails from unverified sources, inappropriate use of passwords, usernames, or system updates might lead to security flaws. Furthermore, security flaws may involve situations where a database manager might open more firewalls than necessary, encourage excessive

employee privilege, or failure to use encryption where necessary. Warkentin et al. (2016) submitted that corporations need to address system flaws and vulnerabilities to take appropriate security actions required to minimize situations that might lead to system compromise. Therefore, database managers need to take proactive measures to address flaws and vulnerabilities that might exist within healthcare database systems to minimize data breaches.

Additionally, threat assessments and coping considerations have been employed to determine behavioral intentions by system users when adopting security measures (Tsai et al., 2016). Security behaviors or perceptions that individuals will act appropriately when using organizational computer infrastructure are yet to be determined. For example, when industries embark on safety measures, such as system audits, IDSs, or routine updates of anti-virus software programs, the belief is that such actions could help in identifying system weaknesses. Surprisingly, the frameworks used in identifying and predicting threat assessments are complicated since cyber attackers develop new ways to diminish systems assurance daily. However, threat assessments could help database managers in identifying potential threats, determine the seriousness of an imminent breach, including developing intervention plans to minimize such violations. Tsai et al. (2016) found that threat assessment and coping considerations are significant predictors when assessing behavioral intention in protecting systems infrastructure. Thus, threat assessments and coping concerns are indispensable when considering different security strategies. Such strategies are essential in developing inclusive security strategies used to protect database systems from security breaches.

Security Strategy Conceptual Model

The critical theory discussed in this section is the integrated system theory of information security management. Hong et al. (2003) developed an integrated system theory of information security management. Hong et al. used the concept to provide a productive information security strategy and methods for researchers, providers, and users to understand information security regarding different perspectives. Hong et al. developed the concept in reaction to the unprecedented security threats posed by cyber attackers and unauthorized users. The central ideas from the theory include (a) security policy, (b) risk management, (c) internal control, (d) information auditing, and (d) contingency management. The theory is useful in building a comprehensive model of information security management that could help database managers to address security issues that might result from inadequate security system management. Scholars indicated that integrated systems theory of information security management is an inclusive framework and a useful managerial measure that could be used to elevate an organization's security (Hong et al., 2006; Young & Leveson, 2014). Integrated system theory of information security management could be useful in capturing relevant concepts necessary for understanding different information security strategies regarding different perspectives, including a combination of security measures database managers may utilize to overcome security threats posed by cyber attackers.

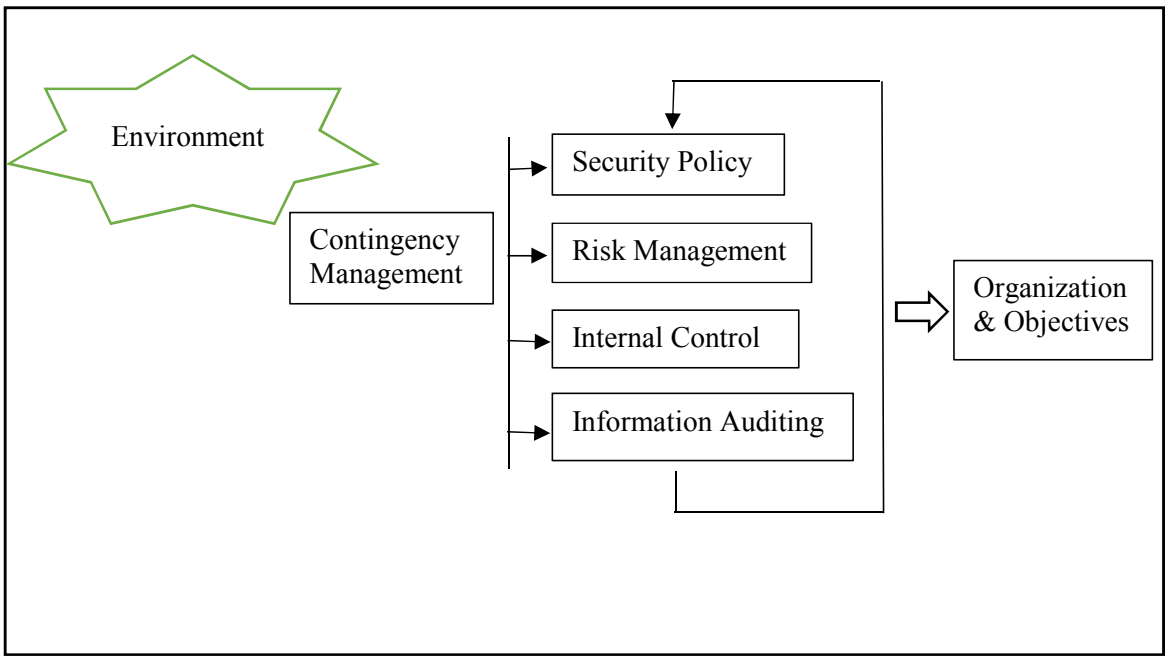

Figure 1. Integrated system theory of information security management. Adapted from Hong et al. (2003).

Security policy. Hong et al. (2003) theorized that security policy focuses on planning information security requirements, including drafting and implementing a security policy to meet security demands in organizational safety requirements. Security policies define how users of information and technology resources may act to prevent, detect, and respond to security incidents (Bauer, Bernroider, & Chudzikowski, 2017; Cram, Proudfoot, & D'Arcy, 2017; Han, Kim, & Kim, 2017). According to Hong et al. (2003), users' compliance with security policy is crucial since policies may include guidelines geared towards protecting organizational data throughout its lifecycle. Such guidelines include procedures for storage, modification, including prevention of unauthorized access, or disclosure of sensitive data. Thus, security policies such as

employee behavior, encryption policy, password, or email user policy, are indispensable to meet organizational safety requirements.

Violations of security policies by employees continue to generate high anxiety. These anxieties are often found to be due to poor security policies (Hong et al., 2003). A review of academic literature points to increased violations of security policies and non-compliance by employees (Eranova & Prashntham, 2016; Flowerday, & Tuyikeze, 2016). Security policy compliance relates to operational guidelines used for maintaining data ordering, safekeeping, and consistency within organizational systems infrastructure (Sicari, Rizzardi, Miorandi, Cappiello, & Coen-Porisini, 2016). While compliance with organizational security policies is required to fight data breaches, Ifinedo and Usoro (2016) argued that employee failure to comply with corporate security guidelines could leave industries vulnerable against system attacks. Thus, developing properly thought-out security policies may help organizations confront violations of such procedures by employees.

Few employees comply with organizational security policies. According to Chen et al. (2018), corporate investigational evidence submits that employees infrequently comply with security policies. Bauer et al. (2017) argued that employees are perceived as more of a threat to organizational security policies. Karlsson, Hedström, and Goldkuhl (2017) maintained that having a plan in place does not necessarily guarantee information security since employees' poor compliance with information security policies is a perennial problem for many organizations. Employee compliance with security policies may include not opening emails or attachments from unknown sources, not divulging

confidential information to social engineers, not sharing of username or password with colleagues, or performing unauthorized updates over organizational healthcare database systems. Thus, employee compliance with security policies is crucial in minimizing information security incidents.

A security policy defines a set of rules and policies regarding employee access and the use of organizational information resources. Sohrabi Safa, Von Solms, and Furnell (2016) outlined that policies alone cannot guarantee a secure system; instead, human aspects of information security should be taken into consideration since the lack of information security awareness, ignorance, negligence, mischief, and employee resistance can undermine corporate security policies. Organizational policies regarding the use of email, password, username, including other applicable guidelines regarding the use of computer applications, may alter employee behavioral attitudes towards compliance with industry security policies. Without employee compliance, security policies may not be able to protect information resources. Additionally, Sohrabi Safa et al. investigated different aspects of organizational security policies and discovered that non-employee security policy compliance might put information assets at risk.

Previous studies revealed that employees' information security compliance plays a vital role in mitigating the risk associated with security breaches (Abawajy, 2014). Non-compliance with organizational security policies might involve inappropriate information security behavior such as opening unknown emails or downloading infected files against corporate regulations. Furthermore, Hwang and Cha (2018) argued that lack of information security awareness or knowledge among staff could be explained by

inadequate education or programs provided by organizational leaders. Whereas system security policy cannot fully guarantee a secure database environment, employee non-compliance with security policies is a challenge for industries.

Risk management. Hong et al. (2003) asserted that risk management identifies security risks and provides a profile to build plans to manage risks. Hong et al. suggested that through organizational risk analysis and evaluation, the threats and vulnerabilities regarding information security could be estimated and addressed. Akinwumi, Iwasokun, Alese, and Oluwadare (2017) gathered that risk management could reduce potentially harmful system threats. Furthermore, Shameli-Sendi, Aghababaei-Barzegar, and Cheriet (2016) argued that the protection of information systems is the first process in the security risk management approach. While risk assessment is a good security approach, it may not result in the elimination of all risks but is effective for determining and understanding risk, including implementing appropriate security measures to reduce risk to an acceptable level (de Gusmão, e Silva, Silva, Poleto, & Costa, 2016). Thus, risk management could help database managers in identifying system weaknesses and vulnerabilities that may comprise healthcare database systems.

Risk identification is a critical activity in organizations and is crucial for the management of organizational information systems (Hong et al., 2003). Dadsena, Naikan, and Sarmah (2016) and Yang et al. (2016) gathered evidence that the identification of risk factors including, the development of risk response plan, is an integral part of a risk management process. Risk management represents a methodical process of identification, analysis, evaluation, and response to risk situations that could undermine systems

assurance (Rodríguez, Ortega, & Concepción, 2017). Preliminary studies indicated that risk needs to be monitored to ensure that the changing environment does not alter risk priorities (Mitchell, 2015). Monitoring a systems' risk is indispensable since identifying vulnerabilities and hazards help to mitigate risk. Risk identification needs to be continuous. Otherwise, the presence of systems exposure could trigger negative consequences for a healthcare organization and could hinder it from achieving its business objectives. While some organizations may not pay attention to risk identification, the benefit is crucial for managing database systems.

Risk management may identify, evaluate, including prioritizing risks or vulnerabilities that could exist within healthcare databases. Hong et al. (2003) stated that the goal of risk management is to bring information security risk at an acceptable level. Yang et al. (2016) argued to bring a security risk to an acceptable level; risk management solutions need to focus on analyzing vulnerabilities and threats to database systems including, deciding what countermeasures could be applied. Such measures may involve security assessment, including appropriate procedures such as audits, or virus protection mechanisms to counter system threats to organizational systems infrastructures. Due to data breaches, risk management is an essential aspect in the development of healthcare databases. Risk management is needed to efficiently identify and respond to various risks faced by organizations since such risks can create a negative impact (Soltanizadeh, Abdul Rasid, Mottaghi Golshan, & Wan Ismail, 2016). Therefore, taking appropriate risk assessment measures could help database managers address system risks within its computer infrastructure and possibly reduce systems risk to a satisfactory level.

The risk of unauthorized disclosure or modification of data can impact an industry in different ways. Risks of unauthorized disclosure or alteration include compromising data confidentiality, integrity, and availability (Rahimian, Bajaj, & Bradley, 2016). Vincent, Higgs, and Pinsker (2017) argued that risk should be appropriately managed so that organizations can effectively guarantee systems assurance. To manage risks, organizations need to identify, assess and prioritize risks, including engaging in a coordinated effort to monitor, minimize, including controlling situations that may lead to system exposure (Vincent et al., 2017). Risk management is essential in addressing security flaws and may involve understanding different types of system risks, including strategies to identify systems modification. For example, unauthorized modification of a database system can lead to undesirable consequences and could impact systems integrity. Whereas risk management helps industries to identify risks, Rahimian et al. (2016) found that unauthorized modification of organizational documents can adversely affect an organization's daily operations. Therefore, risk management is indispensable in protecting database systems from data breaches since a breakdown in risk management could affect internal database controls, which may lead to the risk of unauthorized disclosure or modification.

Internal control. Preliminary studies highlighted that internal control helps in preventing, directing, and correcting illegal events. Hong et al. (2003) theorized that organizations should establish information control systems, and after its implementation, auditing procedures should be conducted to measure the control performance. Internal control is imperative for monitoring users' activities within organizational database

systems. Internal control can monitor employee activities, including initiating preventative measures and correcting illegal activities. An effective internal control provides a real assurance that policies, tasks, procedures, performances, and other aspects of security mechanisms could ensure compliance with organizational goals and objectives (Rahimian et al., 2016). Internal controls represent an essential security strategy. Internal controls, for example, can monitor how a healthcare database system resources are directed; it can detect and prevent intrusive activities initiated by cyber attackers, including checking illegal employee behaviors that might put the organization's database system at risk. Thus, through the implementation of internal controls systems, organizations could measure systems performance.

Organizations need effective IT governance. IT governance must meet the need for security measures relating to internal control systems (Haislip, Peters, & Richardson, 2015). Past corporate breach experiences, including global financial theft, demonstrate the importance of internal control systems (Rubino, Vitolla, & Garzoni, 2017). Internal controls make it harder for attackers to break into the organizational system and limit the damage if a system is attacked (Sampemane, 2015). With internal control in place, one phished password will, at most, get a cyber attacker what a system user has access to, not necessarily everything within the internal network. Internal control can monitor database system resources, detect and raise alerts against illegal intrusions, prevent data breaches that may result from the activities orchestrated by cyber attackers, including monitoring employee system compliance or violation against organizational database policies. Whereas internal control is indispensable in the

organizational security system, security, a breakdown in internal controls could be detrimental to corporate security infrastructure. Thus, with effective internal control systems, database managers could evaluate database applications, monitor who does what, and when, check for system violations and, in so doing, makes it difficult for cybercriminals and illegal system intruders to break into organizational databases.

As a result of numerous data breaches, the importance attached to internal control has increased (Lawrence, Minutti-Meza, & Vyas, 2018). Controls may refer to relevant measures designed to ensure that the system's infrastructure is well managed (Lawrence et al., 2018). Such measures may include firewalls, anti-virus software, or IDSs designed to protect systems from unauthorized use, modification, disclosure, disruption, or destruction (Cavusoglu, H., Cavusoglu, H., Son, & Benbasat, 2015). While Lawrence et al. (2018) claimed that internal control could either prevent security violations before they arise, or detect security violations as they occur, Cavusoglu et al. found that such measures may not prevent social engineering attacks since they use social skills to convince gullible users to initiate a breach through revealing passwords, usernames, or other identifying information. Internal control requires security awareness programs to enable users to recognize security concerns that may jeopardize organizational security assurance (Cavusoglu et al., 2015).

Cavusoglu et al. stated that awareness programs might encourage users to change inappropriate behavior, including adopting decent security practices. Furthermore, Otero (2015) contended that awareness programs could prevent security violations that may result due to employee negligence, error, or actions that stem from malicious activities.

For example, a security awareness program in a healthcare industry may involve assembling a security awareness team, engaging in appropriate security training, including communicating awareness programs within the organization. Cavusoglu et al. (2015) concluded that security awareness programs are imperative in addressing security situations that may jeopardize origination's information system. Awareness programs are crucial in adopting responsible security practices, and such practices may involve information auditing, which could be used to examine or measure systems controls within a database infrastructure.

Information auditing. Information auditing is a procedure conducted to measure systems performance (Hong et al., 2003). Mercuri and Neumann (2016) gathered evidence that industries depend on auditing for evaluating security flaws, insider misuse, including systems performance. For example, whenever an employee performs non-routine access, such as troubleshooting or debugging, such usage needs to be audited to ensure the individual did not deviate from organizational security procedures. Auditing is necessary for estimating system status, discovering risky areas, and levels of risk, including providing recommendations for the improvement of system governance (Drljača, & Latinović, 2016; Haislip, Peters, & Richardson, 2016). Thus, the measure is necessary for evaluating several activities within the network to assess systems performance and could help database managers to measure internal systems behavior.

An information audit evaluates management controls. Such audits determine if information systems operate efficiently, including maintaining systems reliability (Drljača & Latinović, 2016). Drljača and Latinović (2016) argued that auditing evaluates

the design and effectiveness of system security through the deployment of the organization's internal controls. Rahimian et al., 2016; Rikhardsson and Dull (2016) found that through systems' audits, information managers could detect unauthorized system modification, including taking proactive actions to address lapses within systems security. While auditing evaluates system controls to check if it is operating efficiently, some scholars have suggested that auditing could be riddled with the risk of overlooking external systems flaws, especially if the focus is on internal auditing (Mercuri & Neumann, 2016). Thus, the audit could be relevant in mitigating risk, including the verification of account logs. Consequently, in a healthcare database system, the method could perform vulnerability security checks, review the application and operating system access controls, including checking for system irregularities to guarantee system reliability.

Additionally, the user's illegal computer actions could undermine the systems audit (Li, Chan, & Kogan, 2016). Illegal activities could be unauthorized system modification or unethical use of passwords or usernames. To investigate illicit actions, system audit could gather security events regarding systems performance, including ensuring the reliability and availability of systems assurance. To be effective in achieving the required results, information auditing needs to collect evidence to determine whether a system of electronic applications have established and implemented adequate audit controls (Li et al., 2016). For instance, in a healthcare database system, a database manager may perform an audit to check that individuals without authorization to access information do not obtain it; check which database was impacted, including who

performed the operation and when? Thus, irrespective of systems audit, user's illegal actions can undermine systems audit and make such systems vulnerable to cyberattacks.

Contingency management. Hong et al. (2003) stated that contingency management is meant for the prevention, detection, and reaction to security threats, vulnerabilities, or systems weaknesses within or outside of an organization. Hong et al. contended that to meet the demands of a fast-changing environment, IT specialists need to examine one or more information security management measures, such as security policy, risk management, control, and auditing, including system management. Hong et al. argued to overcome security threats, one must combine two or more security measures. Simab, M., Chatrsimab, Yazdi, and Simab, A (2017) agreed with Hong et al. that contingency management strategies must combine several security measures to build a robust security management system to overcome different security threats. Such threats may result from inadequate security policies, audits, or internal controls. Thus, integrating various security measures is imperative for detecting system threats and vulnerabilities.

Technical Strategies

Authentication. Authentication establishes that the subject is actually, what he/she is (Kumari & Om, 2015; Yevseiev, Kots, Minukhin, Korol, & Kholodkova, 2017). Authentication mechanisms guarantee the safety of data against security breaches, such as information manipulation or impersonation (Bonneau, Harley, Van, Oorschot, & Stajano, 2015). Kumari and Om (2015) explained that authentication provides an additional layer of protection against security breaches and focuses on determining if a

person is who he/she claims to be through the use of a password, username, or fingerprint. Liu, Lyu, Wang and Yu (2017) contended that the authentication scheme, which remains the most popular form of verification, has been identified to be insecure and vulnerable to guessing, dictionary attack, key-logger, shoulder-surfing, and social engineering. Irrespective of the fact authentication scheme has been determined to be insecure; the measure can check for the correctness of user identification through a series of identification mechanisms before validating who a user is. Thus, the mechanism is crucial in verifying who an individual is, including protecting systems from cyberattacks.

Regardless of the ease of deployment, passwords are exposed to various types of cyber-attacks. Khedr (2018) explained that to guarantee authentication, system users choose their usernames, including passwords, when registering different accounts to safeguard privacy. However, passwords are vulnerable to compromise through the use of various forms of information tapping like Keylogging, phishing attack, human shoulder-surfing, or camera-based recording (Liu et al., 2017). For instance, a typical healthcare organizational database system could have passwords for many purposes, such as logging into accounts, accessing system applications, retrieving emails, or accessing secure files. Accordingly, no single technology is likely to solve authentication entirely in all cases (Bonneau et al., 2015). Whereas no unique technology can seamlessly solve authentication issues, passwords which serve as an authentication mechanism could also be susceptible to cyber-attacks.

As a result of flaws and weaknesses associated with traditional authentication mechanisms, new methods have been introduced. Investigators have suggested the use of

a two-factor authentication measure to prevent security breaches (Zhang, Tang, Chen, & Zhu, 2015). Zhang et al. explained that a two-factor authentication provides a robust and efficient authentication measure since it utilizes what a person knows and what a person has to establish mutual authentication. Furthermore, to ensure privacy, organizations may introduce the use of a smartcard. Such usage could eliminate keylogging attack through the avoidance of keystrokes or onscreen keyboard. Healthcare industries may employ two-factor authentication to secure patients' privacy through the application of a users' password and smartcard. Through two-factor authentication, a system user can be viewed as a trusted user after the individual has provided vital pieces of identifying information. Therefore, two-factor authentication could help prevent system weakness and possibly protect it from data breaches. The wireless network faces several network attacks and may not be defended by two-factor authentication (Wu et al., 2018).

The security of such networks remains a top priority for healthcare organizational databases. In some cases, the impact could have drastic consequences, brutally affect organizational security and possibly lead to system paralysis (Wu et al., 2018). Jiping, Yaoming, Zenggang, and Shouyin, (2017); and Zhang et al., (2015) noted that security mechanisms like authentication, which organizations use to verify a user through wireless networks, might face several security challenges. Jiping et al. (2017) argued that such measures could be vulnerable to several attacks such as offline password guessing attack, frequency-based attacks, user impersonation attack, sensor node attack, and gateway node bypassing attack. Wireless networks could pose serious security threats to healthcare database systems since the signals attached to these networks are spread in the

air, making it easy for cybercriminals to intercept such signals. Whereas two-factor authentication provides strong authentication, its ability to protect wireless sensor networks from system attacks could be difficult.

As a result of system flaws attributed to two-factor authentication schemes, investigators have resorted to three-factor authentication schemes to add an extra layer of protection due to data breaches (Jiang, Khan, Lu, Ma, & He, 2016). Jiang et al. (2016) argued that a three-factor authentication combines a password, smart card, and biometrics to provide a higher security strength. The mechanism requires multiple authentication factors such as a password; or a possession factor involving something only the user has like a mobile phone number; or an inherence factor suggesting something only the user is such as biometrics. Healthcare organizations and businesses may rely on multiple authentication measures to protect systems infrastructure from security breaches since such measures have been known to protect organizational systems infrastructure from security threats initiated by cyber attackers (Shaji & Soman, 2017). Thus, breaching multiple-factor authentication is a daunting task for cybercriminals, even if such attackers manage to circumvent the users' passwords. Shaji and Soman (2017) argued that in three-factor authentication, a user might not have access to systems infrastructure until such individual has satisfactorily presented verifiable pieces of evidence to an authentication measure.

The use of a three-factor authentication is necessary based on the fact an unauthorized player will not be able to provide critical pieces of identifiable evidence needed for the system's access. In three-factor authentication, if one of the crucial pieces

of evidence is missing, the user will not have access (Haoxing, Fenghua, Chenggen, & Yalong, 2015). As a result of widespread breaches against healthcare industries, including unauthorized disclosure of personal medical health information, three-factor authentication access for a healthcare database may require an employee to provide a username, a password, including a badge swipe for proper identification. Hence, a three-factor authentication mechanism is imperative for securing systems.

Additionally, scholars suggested that a three-factor authentication can provide a fundamental safeguard against illegitimate access to system applications (Dasgupta, Roy, & Nag, 2016; Shaji & Soman, 2017). As a result of privacy breaches across the globe, protecting critical computing systems from unauthorized access is a significant issue forcing organizational leaders to consider three-factor authentication as a viable option (Dasgupta et al., 2016). Park, Y., Park, K., Park, Y., Lee, and Song (2017) noted that in contrast with passwords, biometrics such as fingerprints or palm prints are unique identifiers and are difficult to be stolen, replicated, or spoofed. Although different forms of authentication are at risk of data breaches, three-factor authentication can guarantee that an impersonator will not be able to provide a correct biometric. Dasgupta et al. (2016) found that three-factor authentication that includes passwords, usernames, barcodes, or biometrics could provide a dependable defense against unlawful access to private data.

Intrusion detection system. An IDS provides critical support to protect organizations from security threats posed by cyberattacks (Al-Yaseen, Othman, & Ahmad Nazri, 2016). Security breaches can affect patient safety or lead to the wrong

diagnosis without the presence of an IDS that monitors system networks against malicious activities (Al-Yaseen et al., 2016). Ikram and Cherukuri (2016) argued that IDS are essential for providing security to different databases, including identifying and tracing network intruders. IDS could utilize information collected from the systems' network to detect malware or attacks against organizational applications (Al-Yaseen et al., 2016; Sharma, Parveen, & Misra, 2016). Intrusion detection systems in a healthcare database can provide critical support to protect corporate data from data breaches. It can detect the presence of malware, virus, illegal system alteration, malicious activities, or organizational policy violations.

An IDS is imperative for monitoring network traffic. The systems can check the activities of intruders who exploit system weaknesses to attack industries (Derhab & Bouras, 2016). Derhab and Bouras (2016) demonstrated that IDS could build a profile of normal behavior, including identifying patterns or activities that deviate from the standard profile. Such profiles might include an analysis of network traffic, system logs, or user logs to determine whether such data contain malicious activities. Sharma et al. (2016) and Saravana Kumar, Deepa, Marimuthu, Eswari, and Lavanya (2016) argued that IDSs could monitor network traffic, and analyze such traffic, including known attack signatures already stored in the systems knowledge base. While Hajamydeen, Udizir, Mahmod, and Abdul Ghani (2016) disputed that current intrusion patterns used by cybercriminals are difficult to detect when it has to do with unknown attacks. Database managers may use the mechanism to monitor system traffic; the activities of intruders

who exploit system weaknesses, including the activities of legitimate system users such as organizational employees, vendors, or contractors.

To enhance the IDS, scholars have considered anomaly-based detection methods as a better approach to protect databases from security breaches (Al-Yaseen et al., 2016). While IDSs can examine computer systems for intrusive activities, they are unable to protect such networks from unknown attacks (Hajamydeen et al., 2016). For example, database managers may utilize anomaly-based intrusion to analyze data collected from various sources such as network traffic, system logs, and user logs to identify whether such data contain patterns attackers may use to breach database systems. Anomaly-based intrusion detection mechanisms within a healthcare database system may protect the system by checking for system behaviors that may fall outside the standard system accepted practice. Thus, Hajamydeen et al. (2016) concluded that anomaly-based detection method is critical for protecting database systems from data breaches.

To better protect systems infrastructure, researchers have proposed the use of signature-based detection to prevent network attacks (Cohen, Nissim, & Elovici, 2018). The measure is a crucial factor in limiting and lowering security attacks in a large-scale network environment. Reducing security attacks to an acceptable level is a significant priority for most organizations, and as a result, signature-based detection could monitor system activity; generate alarms, including reporting security violations through the use of database known attack signatures. Amongst healthcare database systems, such mechanisms may contain specific information regarding what attack is detected, the extent of the attack, including possible damage to the systems' infrastructure. Database

managers could utilize such measures to initiate security actions within organizational database systems to determine which system areas may be vulnerable.

Network users face several cyber threats such as malware, data breach, phishing, including social engineering (Bajtoš, Gajdoš, Kleinová, Lučivjanská, & Sokol, 2018). Zheng, Cai, Zhang, Wang and Yang (2015) asserted that the network IDS might be utilized to surmount several network attacks by monitoring the network against malicious activities. Network IDS could minimize attacks initiated by cybercriminals, including preventing a vast array of malicious intrusions that could potentially save organizations tens of billions in losses (Zheng et al., 2015). Database managers could utilize network IDSs to analyze incoming traffic such as emails or files from employees, vendors, or contractors, including investigating malicious intrusions that might originate from cyber attackers. Whereas the mechanism may be vulnerable to advanced malicious attacks such as IP address spoofing, encrypted payload, or human failure, the mechanism could be used to protect healthcare database systems from intrusive activities initiated by cyber attackers.

Encryption. Encryption provides robust data security, including protecting organizations from the disclosure, or leakage of private data (Thomchick & San Nicolas-Rocca, 2018; Zhou, Chen, Zhang, Su, & James, 2019). Thomchick and San Nicolas-Rocca (2018) explained that the encryption mechanism aims at keeping sensitive information confidential while it is being transmitted or stored on a medium that could be potentially subject to unauthorized access. Due to the wide range of data breaches against various computer infrastructures, industries, and several organizations implement

encryption mechanisms to ensure data privacy, including preventing attacks from both outside intruders and malicious inside users. For example, encryption could defend healthcare industries from cyberattacks, including protecting it from against frequency-based attacks. Hence, encrypting data could provide vigorous security against the disclosure of private data.

To enhance encryption, scholars have identified asymmetric encryption as a mechanism to guarantee extra security for private data (Dai, Li, & Zhang, 2016). Di, Li, Qi, Cong, and Yang (2017) asserted that asymmetric encryption requires a public key for encryption, including a corresponding private key for decryption, which is known only to the owner. In asymmetric encryption, a user could secure data by encrypting a message using a receiver's public key, while such a message may only be decrypted with the receiver's private key (Di et al., 2017). Asymmetric encryption algorithms could provide extra security since it involves two parties: one party as sender *encrypter* and the other a receiver *decrypter* (Chen, Tuan, Lee, & Lin, 2017). However, Run-hua, Hong, Jie, and Shun (2015) found that asymmetric encryption, when applied to multiparty-oriented environments, may experience serious security issues due to overload, including the ability to manage multiple keys. Irrespective of security issues, database managers may utilize asymmetric encryption to accomplish authentication if the public key can verify that the holder of a paired private key sent the message. Thus, the measure is vital for securing system applications.

Baykara, Das and Tuna (2017) argued that symmetric encryption guarantees data privacy, including deterring illegal data accesses. The mechanism can provide stronger

security measures since it uses a single key to encrypt and decrypt decode (Baykara et al., 2017). Baykara et al., 2017; Poh, Chin, Yau, Choo, and Mohamad (2017) demonstrated that the mechanism plays a vital role in security assurance since it can guarantee a system with not only confidentiality, but authentication, integrity, and non-repudiation. Furthermore, symmetric encryption is one of the essential techniques in cloud computing, and unlike traditional encryption, symmetric encryption is based on the assumption that the data owner holds a secret key that is unknown to the adversary (Dai et al., 2016). The approach may be critical in protecting database systems because the measure can guarantee data privacy, prevent illegal interception of files by cybercriminals, including protecting systems infrastructure from data breaches.

Additionally, while encryption is an indispensable security mechanism in securing data, law enforcement officials, including government agencies, worry about the probable impact of encryption and believe restrictions are necessary (Bay, 2017). As a result of cyberwar waged by cybercriminals, computer experts stress that restrictions to weaken encryption could be more harmful than helpful (Bay, 2017). For example, the U.S. government expressed disappointment over the role of allowing encryption in commercial products. The primary concern about restricting encryption in commercial products is the possibility of criminals, and predominantly terrorists, or child pornographers hiding evidence of illegal activities from authorized investigators (Spafford, 2016). Recently, the terrorist event in San Bernardino raised new issues about the encryption of personal devices such as smartphones and tablets (Spafford, 2016). While encrypting these devices may prevent law enforcement agents from accessing

information from such devices during an investigation, not encrypting sensitive data may lead to information exposure.

Data Breaches

A breach is unauthorized access or compromise of personal information such as names, dates of birth, or social security number (Sen & Borle, 2015). The breach may involve the intentional or unintentional release of secure information to untrusted individuals. A data breach is a significant threat to the United States economy. It is one of the manifestations of the continually evolving field of cybercrime. Unlike identity theft, data exposure could result in the public disclosure of private information (Agelidis, 2016). Hacks involving the disclosure of private information could result in the reputational harm of victims, causing industries billions in losses.

A data breach can hurt businesses and consumers in different ways. For example, about five million U. S. clients lost resources averaging $351 due to data breaches (Arachchilage, Love, & Beznosov, 2016). Such a compromise could occur due to inadequate coding, which could threaten systems security assurance (Murtaza et al., 2016). For example, the number of attacks exploiting system weaknesses increased to 142 million in 2014 from 83 million in 2013 and 34 million in 2012 (Murtaza et al., 2016). In a data breach incident, sensitive or protected information, for example, in a healthcare system, maybe illegally viewed, stolen, or used by an unauthorized individual to harm the industry. The breach may involve the theft of personal health information, trade secrets, financial information such as bank account numbers, or intellectual property either to steal or cause damage to the systems' infrastructure.

Databases are highly lucrative targets for hackers (Kar, Panigrahi, & Sundararajan, 2016). Kar et al. (2016) gathered evidence that some databases are built with open source packages, including third-party plugins without proper verification of software coding. As a result of poor coding, database applications are fraught with multiple weaknesses, which an attacker could exploit to breach systems (Kar et al., 2016). Cybercriminals could take undue advantage of database weakness to undermine systems assurance, thereby leaving such applications vulnerable to attacks (Kar et al., 2016). Due to database weaknesses, hackers could exploit system errors, circumvent defense systems, including compromising sensitive information, which could lead to data breaches. Whereas databases are vulnerable to security attacks, it is crucial to protect such systems from adverse situations that may lead to security breaches.

A data breach is a significant security challenge for several industries. While afflicted organizations incur substantial financial losses, such industries equally suffer the cost of providing a financial remedy to victims, including meeting legal liabilities (Gwebu, Jing, & LI, 2018). Researchers have sought to quantify the economic cost associated with data breaches, including finding technical strategies to develop adequate preventive controls. Regardless of the level of apparent security controls, a critical practical lesson is that complete security risk prevention could be difficult for healthcare organizations to achieve. Malicious outsiders could take undue advantage of system vulnerabilities and weaknesses to launch a significant security assault against healthcare industries (Sen & Borle, 2015). As a result of tremendous financial losses suffered by healthcare organizations through the theft of personally identifiable information, database

managers need to find security strategies used to respond to data breach incidents to minimize the economic losses suffered by industries as most businesses are conducted online.

Data breaches resulting from online shopping pose a significant challenge to corporations as it may lead to the exposure of personal information (Alhouti, Johnson, and D'Souza; Chakraborty, Lee, Bagchi-Sen, Upadhyaya, & Raghav Rao, 2016). Recent evidence has demonstrated that more than 70% of merchandise purchased online are frequently completed through credit card payments (Chakraborty et al., 2016). While e-commerce has witnessed tremendous improvements, Alhouti et al. (2016) contended that trust and privacy concerns had sustained a remarkable interest, given the risks associated with online shopping. In online shopping, consumers can directly buy goods and services from a business over the internet using a web browser. Online shoppers could face a higher risk of fraud from cybercriminals who could break into the organization's website to steal names, addresses, and credit card numbers. While online shopping is an essential part of today's economy, such a method could lead to the exposure of personal information.

Scholars have identified insiders as the weakest link in organizational computer assets (Dang-Pham, Pittayachawan, & Bruno, 2017; Manworren, Letwat, & Daily, 2016; Walsh & Miller, 2016). Manworren et al. (2016) stated that employees accounted for 59% of security incidents. Across several United States companies, unauthorized use of computers by employees accounted for $40 billion in losses (Manworren et al., 2016). One way to reduce the possibility of a data breach is to understand security strategies,

including employee compliance behaviors (Manworren et al., 2016). Healthcare organizations, for example, could take extra measures to protect its network from external threats, but it might become a daunting task for such organizations to protect itself from insiders due to the fact insiders have knowledge and access to systems infrastructure. Thus, insiders could pose the biggest internal threat to organizational databases.

Edward Snowden, the American whistle-blower, is a typical example of an insider. Snowden's destructive leaks compromised national security by copying and leaking highly classified information (Walsh & Miller, 2016). His disclosures revealed numerous surveillance programs. Because of insider leaks, organizations may deploy tools that could utilize algorithms to profile employee computer actions to distinguish between normal and abnormal behaviors. Apart from technical tools, comprehensive information security programs might help to build an information security culture in which a collection of security values, norms, and knowledge could help in enhancing security measures. Whereas, insiders might change their behavior if information security becomes a top priority for organizational leaders, the benefit outweighs the risk of security compromise perpetrated by insiders.

Data breaches are becoming more damaging to many businesses due to the activities of cybercriminals. The Target data breach, for instance, marked the beginning of increased scrutiny of cybersecurity practices (Manworren et al., 2016). The United States Congress has considered a plethora of cybersecurity and data breach laws as it assesses the framework of the current cybersecurity environment (Manworren et al., 2016). Unfortunately, significant gridlock in Congress could delay the progress of such

legislation. The absence of federal regulation may encourage cybercriminals to behave in inappropriate ways forcing large businesses to pass millions of dollars in data-loss-related expenses to credit card companies, insurance companies, and consumers (Manworren et al., 2016). Consequently, the lack of uniform federal regulations also means that businesses operating in multiple states must comply with local laws and regulations. Thus, healthcare organizations have the responsibility of safeguarding private data and making sure that databases exposed to web systems are secure enough to withstand illegal activities initiated by cybercriminals.

Web systems commonly face a unique set of security threats due to inadequate safety measures. Movahedi, Cukier, Andongabo, and Gashi, (2019) gathered that security threats from such applications could result in system faults, including high exposure or access by browsers. Therefore, predicting system vulnerabilities could provide a metric for early detection, including providing technical strategies for organizations to decide how to respond, prepare, and plan for cyber incidents (Sampaio & Garcia, 2016). With web systems, it is possible to stream sophisticated images, including delivering information anywhere in the world. Database managers could use the measure to provide information and services to users. Whereas web systems can provide services anywhere in the world, inadequate security techniques within web systems could permit intruders to gain unauthorized access into systems infrastructure. Therefore, the procedures need adequate security measures to secure such systems from security threats.

Organizations could use risk assessment to measure security risks, including identifying vulnerabilities (Holm & Afridi, 2015). Holm and Afridi (2015) gathered

evidence that risk analysis identifies an organization's valuable information assets, including vulnerabilities, while revealing threats that may take advantage of those weaknesses. Furthermore, Holm and Afridi (2015) found that the Common Vulnerability Scoring System could measure the severity of system vulnerabilities. According to Holm and Afridi (2015), the scoring for all vulnerabilities in the U.S. National Vulnerability Database is in three discrete states: Low severity, medium severity, and high severity. While corporations use risk analysis to identify system vulnerabilities, Ruohonen (2017) argued the measure had been found with problems related to inconsistencies, time delays, and glitches of classification standards. Irrespective of concerns with risk analysis, database managers could use the measure to identify system risk factors that have the potential to cause harm to organizational databases, including mechanisms to address such risk factors.

Furthermore, to identify system vulnerabilities, organizations utilize the skills of ethical hackers. Rafferty (2016) noted that ethical hackers help to identify system vulnerabilities before they become a target of malicious cyber-attacks. Ethical hackers could impersonate the activities of cyber hackers and systematically undertake an attack on the organization's information system to evaluate security (Rafferty, 2016). Through such actions, ethical hackers like designated organizational employees or contractors could test any weaknesses or areas that malicious hackers could potentially exploit. In ethical hacking, also known as penetration testing, healthcare database managers can examine organizations database defenses in the same way a malicious hacker might do to search for system weakness to apply corrective measures before hackers could use it

against such organization. While it is challenging to develop applications free of vulnerabilities, ethical hackers can spot system flaws cybercriminals might utilize to attack system infrastructure.

Types of data breaches. A data breach incident involves unauthorized access to sensitive or confidential data that could result in the compromise of confidentiality, integrity, or availability of data (Sen & Borle, 2015). Sen and Borle asserted that sensitive or confidential data might include personal health information, personally identifiable information, trade secrets, or intellectual property. Sensitive data could be breached or compromised through denial-of-service, cracking of passwords, human error, or phishing (Choi, Kim, & Jiang, 2016). Other types of data breaches involve unauthorized access, malware, hacking, spamming, virus, Trojans, or worms (Zou, Zhang, Rao, & Yi, 2015). A cyber attacker may utilize a worm, which is a malicious program, to breach a healthcare database system. A worm can transmit itself over the network, infect systems network, including undermining systems assurance. Hence, such a breach could paralyze organizational systems' infrastructure.

Malware is one of the significant threats facing computer security. Zou et al. (2015) asserted that malware such as Trojans, viruses, worms, spyware, and botnets pose a severe threat to user privacy, social economy, and national security. For example, the proportion of packed malware is growing exponentially and could comprise more than 80 % of all existing malware (Bat-Erdene, Park, Li, Lee, & Choi, 2017). Attackers continually make malware harder to detect or analyze. Although anti-malware and other elimination tools can mitigate this situation to some extent, the evolution of polymorphic

and metamorphic malware is making the fight against its use more difficult (Bat-Erdene et al., 2017).

Furthermore, due to its damage to systems infrastructure, malware such as viruses, worm, or Trojan have caught the attention of both the anti-malware industry and researchers (Fan, Ye, & Chen, 2016). Across the world, financial losses suffered by different organizations due to malware infection averaged $12.18 billion per year from 1997 to 2006 and increased to $110 billion between July 2011 through the end of July 2012 (Guo, Cheng, & Kelley, 2016). Thus, malware is a significant threat to computer systems and could pose a crucial security challenge for healthcare industries.

A denial-of-service (DoS) attack is an attempt to make a network resource unavailable to its intended users (Behal, Kumar, & Sachdeva, 2018). Behal et al. (2018) and Mazur, Ksiezopolski, and Nielek (2016) asserted that a denial of service attack might refer to a coordinated effort between several machines to attack one or multiple target systems to a point where the server services become unavailable to legitimate users. Such attacks might initiate from multiple ends of a wireless sensor network with the intent of exhausting systems limited resources (Mazur et al., 2016). Denial-of-service attacks could paralyze a healthcare database system, making patients' information unavailable, and possibly introducing vulnerabilities that could enable cyber attackers to unleash data breaches. The attack could inflict severe damage to databases making network services unavailable.

Hackers utilize phishing to carry out data breaches against gullible users. Arachchilage, Love, and Beznosov (2016) gathered that phishing is a cybersecurity theft

which aims at stealing confidential information such as username, password, including other forms of sensitive data from gullible victims. Phishing employs social engineering techniques to trick system users into revealing personal and secret information (Jain & Gupta, 2016). Jain and Gupta (2016) argued that detecting and preventing phishing attacks is a significant challenge since attackers can perform such attacks in several ways to bypass organizational anti-phishing techniques. For example, in a phishing attack, an attacker may create a fake web page by copying or making a minor change to a legitimate page, so that a database user or an employee looking at the web page will not be able to differentiate between phishing and valid web page. Jain and Gupta (2016) found that while industries may integrate security features to raise alerts whenever an internet user accesses a phishing site, such measures may not protect organizations from gullible system users.

Scammers use phishing to target victims into divulging personal information. Most of the victims targeted may involve large industries such as healthcare, banks, or money transfer agencies (Jain & Gupta, 2016). For example, more than 5 million U.S. clients lost an average of $351 to phishing attacks (Arachchilage et al., 2016). In phishing, the attacker could send a large number of spoofed hyperlinks to employees in which case opening the link could redirect the employee to a fake server instead of a legitimate organizational database (Jain & Gupta, 2016). In phishing attacks, an employee can divulge or submit employee ID, username, or password to a fake server, believing it to be a genuine organizational system network. Such actions could lead to

system compromise. Thus, the danger posed by phishing scam is a major challenge for industries.

Cybercriminals use spamming images to commit data breaches through deceiving victims to click on such images (Abulaish & Bhat, 2015). The method uses electronic messaging systems to send an unwanted message, especially advertising (Abulaish, & Bhat, 2015). Abulaish and Bhat (2015) argued that spamming remains a viable option for cybercriminals economically since there are no operating costs involved in sending unsolicited messages to victims in the bid to advertise products or websites. The motive behind spamming may include promoting products, advertisement, viral marketing, and in some cases, harassment of legitimate system users. Criminals could hide malware behind images deceiving gullible individuals to click on it. Thus, cyber attackers could use such clandestine mechanisms to breach the systems' infrastructure.

Furthermore, cybercriminals equally employ random link attack to deceive victims (Abulaish & Bhat, 2015; Ghosh, 2014). Abulaish and Bhat (2015) noted the attack is one of the most common forms of spamming. Abulaish and Bhat (2015) argued the measure involves an arbitrary attack where a small number of spammers could send spam to a large number of randomly selected victims. Such attacks might appear to be legitimate, but scammers could use the scheme to deceive authorized users into creating trusted links, thus breaching their privacy. Usually, the primary motivation behind a random link attack is to circumvent the spam filters, including hiding such messages to deceive gullible users (Ghosh, 2014). Thus, system users need to be aware of the dangers

random link attacks could pose to organizations and how such links might lead to the breach of personal privacy.

Insider breaches. Insider threats have gained prominence within organizational database systems and pose challenging risks to database environments. An insider breach may occur when an employee authorized to perform job responsibilities within an organizational computer system unknowingly or knowingly abuse such privileges to harm systems network infrastructure. With their knowledge and access to corporate resources, insiders could launch attacks that could result in more damaging impacts compared to outsiders (Liang, Biros, & Luse, 2016). An insider is one who can operate within a defined boundary. Boundaries could be national, physical, or logical; or a combination of the physical and logical boundary. While organizations could guard their computer systems against external threats, guarding against insiders is challenging since such individuals are legitimate organizational system users.

Pasquale, Hanvey, Mcgloin, and Nuseibeh (2016) asserted that insider attacks could originate from people within the organization, such as employees, former employees, contractors, or business associates, who have insider information concerning the organizational security practices. Since past employees could possibly maintain elevated privileges, including knowledge and skills of the corporate network system, such individuals may circumvent security measures to either steal or damage valuable organizational data (Jingguo, Gupta, & Rao, 2015). An insider, for example, a healthcare employee, may unintentionally open a phishing or spam emails, click on an infected attachment file, unknowingly divulge a password, or violate organizational security

policies. Such employees may not have bad intentions or malicious motives; however, their actions can generate undesirable consequences for a healthcare database system. Thus, illegal activities by insiders against organizational database systems could produce adverse effects.

Insider attacks may involve violations of operational security, including the misuse of authority (Brunisholz et al., 2015). Such threats might encompass typical coercion schemes employed by cyber-scammers, which could lead to data breaches (Brunisholz et al., 2015). For instance, violations of operational security in a healthcare network may involve opening an email or attachment that does not originate from an organizational network system or making unauthorized changes to the system database. An insider authorized to access system resources but uses them in a way not approved by the organization could cause serious harm, including damaging organizational reputation (Brunisholz et al., 2015; Padayachee, 2016). Since insiders have corporate data accessible to them, they could misuse the trust invested in them to harm organizational systems infrastructure. Thus, a simple misuse of authority by insiders could create serious security consequences for healthcare network systems.

The danger of insider threat is far greater than that of external threats (Liang et al., 2016). Brunisholz et al. (2015) argued that unlike an outside intruder, an insider has the opportunity and privilege to obtain sensitive or classified information, including the ability to know weak points within organizational information systems. As a result of security threats posed by insiders to corporate database systems, scholars like Lu, Sun, Liu, and Li (2018), advocated the use of IDSs to build a user profile, including detecting

a possible deviation and illegal data access within systems infrastructure. While such proactive measures may go a long way in minimizing data breaches, it may not be able to contain the threat posed by insiders due to their knowledge and ability to navigate the systems network system.

Database managers advocate several defense measures such as authentication, IDSs, or encryption to protect systems' infrastructure from insider attacks (Jingguo et al., 2015). However, preventing such attacks is difficult if insiders fail to adhere to organizational system policies (Lu et al., 2018). Behavioral indicators such as corporate policy negligence can provide a probable sign for early warning of malicious intent (Lu et al., 2018).

For example, in a healthcare database system, while authentication can verify the identity of the user, and IDS can monitor a network for a malicious system's activity, and encryption can encode a message so that only authorized parties can view it, the measures may not prevent an insider from opening a malicious file. Hence, defensive measures may not be able to protect organizational systems from all attacks posed by insiders.

Additionally, insider attacks are dangerous due to the fact the attacker can exploit the knowledge of organizational database systems due to the fact an employee may have knowledge of systems weaknesses. Most of the time, defense mechanisms such as authentication, access control, or encryption may not be able to protect systems infrastructure if the insider could navigate systems security mechanisms. Jingguo et al. (2015) and You, Ogiela, Woungang, and Yim (2016) found that such mechanisms may not be able to prevent insider attacks. Attacks initiated by employees who have access to

database infrastructure can be difficult to defend since bad employee behaviors can remain undetected for a long time, thereby leading to data breaches. Therefore, insider threats remain a critical concern for organizational network information.

Victims of data breaches. Data breaches have become a frequent phenomenon causing enormous damages to businesses due to system vulnerabilities (Genge, Kiss, & Haller, 2015; Manworren et al., 2016). Deploying security measures may help in addressing such violations. Target corporation, for example, became a victim of data breach and the security breach against the industry in 2013 resulted in the theft of several million credit card numbers forcing Target to settle a class-action lawsuit for several million dollars; providing $10,000 in relief to customers, including $67 million to Visa, as well as $19.11 million to MasterCard (Manworren et al., 2016). Corporations, including individuals, could become victims of data breaches as a result of the interconnected network, including malicious activities by cyber attackers. Data breaches could destroy an industry's reputation or systems infrastructure, causing millions of dollars in losses, as well as the theft of personal information.

Data breach incidents continue to dominate U.S. headlines with a large-scale of cyber-attack surpassing the probability of natural disasters (Conteh & Schmick, 2016). The former FBI Director, James Comey testified before a Senate Homeland Security Committee that cyber-attacks had surpassed terrorism as a significant domestic threat (Conteh & Schmick, 2016). Comey's testimony is a living testament when compared with other puzzling data breaches. In 2014, Target Corporation's chief executive officer resigned his job after the 2013 Thanksgiving holiday season, when the personal

information of approximately 100 million customers was stolen (Manworren et al., 2016). The attack compromised a range of personal information such as names, addresses, dates of birth, and social security numbers, causing the individuals involved in the compromise hardships and emotional distress. Thus, data breach incidents pose a significant domestic threat.

Consumers, including employees, have become victims of data breaches through the skillful manipulation of human gullibility by social engineers (Conteh & Schmick, 2016). Sometimes, employees do not consider themselves as part of organizational information security. Such thinking may not create security awareness amongst employees or business associates. Siadati, Nguyen, Gupta, Jakobsson, and Memon (2017) highlighted that the idea behind social engineering is to take advantage of employee natural tendencies and emotional reactions. Social engineering, also known as human hacking, is the art of tricking employees and consumers into disclosing their credentials while cybercriminals use such information to gain access to networks (Conteh & Schmick, 2016). Heartfield and Loukas (2015) claimed that social engineering attack aims at manipulating victims into divulging confidential information. Even with the most robust security measures, healthcare organizations could still become victims of cyberattacks. Such is possible if a cybercriminal could successfully manipulate an employee into divulging a password, opening a malicious email attachment, or visiting a compromised website. Whereas safety measures are aimed at improving security systems, Conteh and Schmick (2016) found that manipulation characterizes the scheme social engineers exploit during attacks.

Additionally, cybercriminals have found new ways of directing cyberattacks against national infrastructures such as the power grid, water supply, dams, communication technologies, or chemical plants. Such infrastructures could be vulnerable to cyberattacks since they depend on communication technologies. You et al. (2016) alluded that such infrastructures could be susceptible to attacks as a result of system vulnerability. Finding adequate security measures to detect, prevent, including responding to such attacks is a daunting task (Nandi, Medal, & Vadlamani, 2016; Yoon, Dunlap, Butts, Rice, & Ramsey, 2016). Critical infrastructures such as nuclear reactors, electricity, water, or IT are vital that their incapacitation could have debilitating consequences on national security, health, or the general economy. Since these infrastructures are dependent on communication technologies, cyber attackers could cause severe damages to such infrastructures by injecting false measurements to sabotage their normal operations. While cybercriminals have found new ways to direct cyberattacks against critical infrastructures, database managers need to develop strategies required to fight data breaches.

Strategies to fight data breaches. Organizations face the challenge of fighting data breaches. The losses suffered as a result of a data breach worldwide is overwhelming (Greengard, 2016). Security breaches due to malware cost victims more than $500 billion each year worldwide (Greengard, 2016). The problem continues to deteriorate daily. Greengard (2016) highlighted that the Ponemon Institute's 2015 Cybercrime study found that the cost of digital crime rose by 19%, of which the average annual loss to companies worldwide was $7.7 million. Fighting data breaches is not an easy task. Different

industries like healthcare organizations may develop different strategies such as the allocation of the fund, education, and programs, including other preventative measures such as the use of encryption, authentication, or IDSs to fight data breaches. Irrespective of security strategies, industries could still face the challenge of fighting data breaches.

Different legislations have been enacted to fight data breaches (Sen & Borle, 2015). Such legislations include state and federal laws such as the data breach notification laws, the federal privacy act, or the national security management act to protect personal, financial, or health data (Sen & Borle, 2015). The laws are designed to act as a deterrent against criminals from engaging in criminal activities, including reducing the number of data breaches, as well as notifying victims in the event of a security breach (Schuessler, Nagy, Fulk, & Dearing (2017). The laws include punitive actions that could be taken against cyber attackers who bridge organizational defensive mechanisms to steal private information, which may include credit card numbers, date of birth, or social security information. Both federal and state laws may compel organizations to report data breaches under the threat of legal action. Thus, such legislations could be useful in combating data breaches.

Organizations are beginning to share data breach threat incidents amongst private sector industries (Schuessler et al., 2017). Sharing of information in the event of data breach occurrence could help industries in reevaluating current organizational security strategies, including taking proactive actions to prevent or minimize future data breach occurrence. Safa and Von Solms (2016) found that knowledge sharing amongst organizations could play a significant role in fighting data breaches. Furthermore, Gao,

Zhong, and Mei (2015) highlighted that the U.S. government encourages the establishment of industry-based CERT, Information Sharing and Analysis Centers, Electron Crimes Task Forces, including Chief Security Officers Round Tables. Sharing data breach incidents is vital in creating awareness not only among industries but even individuals. Thus, sharing such reliable information from service providers, commercial security firms, or government agencies could help in reducing the wave of data breaches.

Several nations across the globe have introduced strong legislation and privacy laws. Kirkpatrick (2015) indicated that the U.K., including other European countries, have enacted stringent laws to dissuade perpetrators of data breaches. Such acts include taking punitive actions against non-compliant industries and fining such organizations for failing to prevent a data breach. Furthermore, jurisdictions such as Hong Kong, Singapore, and Australia, including other Asian nations, have introduced more stringent privacy laws (Kirkpatrick, 2015). Whereas such legislations and privacy laws are imperative for protecting private data, it is crucial to match such legislations with adequate security measures to prevent breach incidents.

Additionally, legislation and privacy laws may not be able to prevent data breaches (Sen & Borle, 2015). While laws are necessary, industries need to take proactive actions through the deployment of IDSs, encryption, or authentication to safeguard corporate databases. Moreover, healthcare organizations need to pay specific attention to insiders, implement security measures, and provide training and education, including programs that could enhance network systems. For example, healthcare industries may implement security controls and defenses, including countermeasures to avoid, detect,

counteract, including minimizing security risks that might affect systems databases. Irrespective of preventative measures and strategies such as data encryption or employee training, including regulations enacted by various governments worldwide, it is difficult to find a single privacy law or protective measure that could prevent all security breaches.

Theft and privacy breaches. Organizations face the loss of reputation due to the theft of private data (Choi et al., 2016). A robbery of organizational data may result in unauthorized access, collection, disclosure, and disposal of personal information, including selling of personal data to third parties (Bargh, Choenni, & Meijer, 2016; Choi et al., 2016). For example, in 2013, a healthcare employee was found guilty of using valid credentials to access, steal, including selling patients' records containing medical record numbers, names, and addresses (Ozair, Jamshed, Sharma, & Aggarwal, 2015). A privacy breach against an industry may not only paralyze that industry database or network system but could damage the industry's reputation; mistrust in information sharing, including imposing massive costs on individuals. Thus, organizations might lose the trust it has built over several years as a result of a security breach.

Privacy breaches such as theft, or other forms of compromise of personally identifiable information, including credit card and social security numbers are on the rise (Choi et al., 2016). Choi et al. (2016) stated that Sony's PlayStation network hacking incident affected approximately 77 million user accounts. Such exposure resulted in a class action lawsuit where victims of identity theft claimed up to $2,500 in damages with a total cost exceeding $171 million (Choi et al., 2016). Furthermore, Edward Snowden, while a contractor for the U.S. National Security Agency (NSA), copied up to 1.7 million

top-secret documents in a thumb drive, which he released to the press (Toxen, 2014). Such breach altered the U.S. government's credibility with the American people, including the relationship with other countries (Toxen, 2014). Thus, the theft of privacy could lead to system breakdown, financial damage, including loss of reputation against individuals, industries, or legitimate governments.

Privacy violations may occur for a variety of reasons. Choi et al. (2016) identified several reasons, including cracking of passwords, backdoors, and denial-of-service, including phishing, human error, or forces of nature. Although organizations may implement technical measures to prevent privacy breaches, however, privacy information could leak through unforeseen holes (Choi et al. (2016). For instance, three Call Center employees received payment from third-party vendors to obtain customer information such as names and social security numbers in which the employees accessed more than 68,000 accounts without consumers' authorization and sold the information to third-party vendors (Ruckman & Dhaliwal, 2015). According to Senate Bill Report (2015), forty employees at the Colombian and Philippine facilities violated customers' privacy by obtaining unlock codes for AT&T mobile phones (McKeown & Storm-Smith, 2016). While privacy violations may occur for a variety of reasons, it is difficult to control, primarily when it originates from organizational employees for economic or selfish reasons.

The U.S. Congress has taken several steps to address privacy breach concerns. For instance, the U.S Congress passed the Cyber Security Information Sharing Act as part of the 2016 Omnibus Spending Bill (McKeown & Storm-Smith, 2016). The bill

aimed to encourage information sharing among the federal government and private entities to protect and respond to privacy breaches. To enhance the bill, the Federal Trade Commission came up with new laws. Under the new law, industries whose security networks are breached by hackers are required to notify affected parties (Agelidis, 2016). As a result of new laws, AT&T Services, Inc. entered a $25 million settlement with Federal Communications Commission to settle an investigation into consumer privacy violation at AT&T's call centers in Mexico, Colombia, and the Philippines - a breach that involved an unauthorized disclosure of about 280,000 US customers names, including social security numbers (Ruckman & Dhaliwal, 2015). Thus, such regulations by lawmakers could force organizations into using appropriate strategies to protect private information.

Furthermore, the new regulations would require industries that store personal data on more than 10,000 customers to notify customers within 30 days of a breach (Ruckman & Dhaliwal, 2015). Covered businesses should implement comprehensive consumer privacy, including data security programs appropriate to the size and complexity of covered entities (Ruckman & Dhaliwal, 2015). According to the new legislation, the penalties for data privacy violations could run as high as $5 million, with an additional $5 million possible for willful abuses (Ruckman, & Dhaliwal, 2015). Thus, enforcing such regulations may encourage industries to not only take proactive security measures in protecting privacy information but to do whatever is necessary to prevent security incidents that could lead to a data breach.

Challenges of combating data breaches. Fighting data breaches or prosecuting perpetrators is a daunting task due to its global nature (Agelidis, 2016). Each day, cybercriminals exploit new ways to compromise database systems irrespective of systems' defensive mechanisms. Data breach perpetrators have taken different dimensions. Attackers could either be willful perpetrators or hacktivists whose sole intention is to steal or cause enormous damage to organizational businesses. Such attacks could come in a variety of forms such as viruses, malware, keylogging, Spam, Trojan Horses, and Backdoors, including other illegal activities orchestrated to wreak havoc to organizational network infrastructure. Perpetrators of cybercrime are often very difficult to find since such criminals may reside beyond national legitimate geographical boundaries. Identifying and bringing such cyber attackers to justice could be difficult due to different federal legislation. Whereas charging hackers can pose significant challenges, not having laws in place could create further security problems.

Each year, many organizations lose tens of billions of dollars in economic damages due to the interconnected global network (Makridis & Dean, 2018). Makridis and Dean (2018) highlighted that cybercriminals might attack vulnerable organizational database systems through the use of different attack methods, including taking advantage of system flaws. In a fake antivirus, attackers may disguise malware as legitimate antivirus software to convince gullible users into buying or installing it (Kim, Yan, & Zhang, 2015). For instance, cybercriminals could employ different tactics such as social engineering or keylogging to breach the organizational healthcare database. Whereas industries continue to lose resources as a result of the interconnected network, taking

proactive security measures could help healthcare systems to fight the activities of cybercriminals, including saving resources and money.

Hackers, including cybercriminals, develop new malware daily, and such developments make it difficult to find the right tools to fight it (Lee & Kwak, 2016). Lee and Kwak (2016) claimed that about one million new malware programs are developed daily on average. Detecting or preventing such hardware Trojans is difficult due to the fact the method used to insert them is numerous, and moreover, malicious software could be easily concealed, making them difficult to detect (Wu et al., 2016). The existing security solutions rely on the recognition of known code or behavior signatures, which are incapable of detecting new malware patterns (Zhang, H., Yao, Ramakrishnan, & Zhang, Z., 2016). While new malware is created daily, it could be difficult for industries to find the right tools, programs, or measures to fight them.

The role of database managers. Organizations are dependent on database managers to protect organizational database systems. Industries hire experienced database managers charged with developing corporate policies, workload priorities, or storage configuration (Abdul, Muhammad, A. M., Mustapha, Muhammad, S., & Ahmad, 2014). While database managers deploy security measures to protect organizational systems, cyber attackers engage in a broad range of intrusive actions such as scanning of systems database or the exploitation of other system weaknesses (Durkota, Lisy, Kiekintveld, Bosansky, & Pechoucek (2016). Such actions could subject systems' infrastructure to several network attacks such as denial-of-service attacks (Asghar, Anwar, & Latif, 2016). For instance, in a healthcare database system, a database manager may oversee database

design, test new database, monitor database efficiency, check for a system vulnerability, including making sure the system maintains confidentiality, integrity, and availability. Thus, organizations need experienced database managers with appropriate strategies to protect database systems from data breaches.

Database managers invest an enormous amount of time in securing healthcare databases and making sure they meet security requirements (Stiawan, Idris, Abdullah, Aljaber, & Budiarto, 2017). Such conditions include the prevention of unauthorized disclosure and modification of information or prevention of system penetration by unauthorized individuals (Stiawan et al., 2017). Crafting a database that can achieve substantial security requirements is a daunting task since database systems process significant amounts of data (Fonseca et al., 2014). In healthcare systems, for instance, database managers may probe the organizational database system to search for security flaws and vulnerabilities an attacker may use to exploit security measures. A database manager might evaluate systems audit, encryption, or IDSs to check for systems assurance. Such responsibilities are necessary to meet organizational security requirements.

Database managers develop solutions such as risk analysis to identify the organization's valuable information assets, including identifying threats that might take advantage of systems' weaknesses (Shameli-Sendi et al., 2016). Furthermore, database managers may implement the Common Vulnerability Scoring System to measure the severity of system vulnerabilities (Holm & Afridi, 2015; Serra, Jajodia, Pugliese, Rullo, & Subrahmanian, 2015). For instance, the scoring for all vulnerabilities in the U.S.

National Vulnerability Database is in three discrete states: low severity, medium severity, and high severity (Holm & Afridi, 2015). Thus, while database managers develop solutions to help safeguard the organization's database systems, they have the responsibility to utilize available security mechanisms provided by the national vulnerability database to implement a remedy against system weaknesses.

Database managers execute effective strategies to implement an incident response plan (Midi, Sultana, & Bertino, 2016). Such approaches could contain information on how to prevent attacks, monitor, and detect suspicious activities, including taking appropriate response policies (Midi et al., 2016). Furthermore, Densham (2015) argued that database managers develop defensive mechanisms such as IDSs, authentication, and monitoring solutions that are critical in identifying legal system users, including sounding an early warning to intrusive activities into systems network. Such defensive techniques may help gather alerts, determine actions, including responding effectively to data breach crises. While cyber attackers may launch cyberattacks on database systems, developing an effective response plan could help avert security breaches.

Database managers address system risk in case of a network breach, or other network issues that could affect organizational network operations (Al-Yaseen, et al., 2016; Chen, Yen, & Shu-Chiung, 2015). Chen et al. (2015) stated that risks change over time as the database environment changes through updates. While threats change over time, scholars have argued that through continuous implementation of control and defense measures, risks can be effectively controlled, reduced, or avoided (Chen et al., 2015). While it is impossible to eliminate all risks in a complex database environment,

database managers could mitigate risk to an acceptable degree (Chen et al., 2015). Database managers address critical systems issues and may implement technologies such as firewalls, encryption, antivirus software, or IDSs. While database managers address systems risk, changes like systems uncertainty over time may lead to data breaches.

Assessing existing security systems is the primary task of database managers. Fonseca, Vieira, and Madeira (2014) asserted that database managers might evaluate security apparatus through the injection of realistic vulnerabilities in a web application, including attacking. Such measures could be used to assess the robustness and effectiveness of existing system security mechanisms (Fonseca et al., 2014). Database experts could use such tools to evaluate the effectiveness of IDSs or encryption. Fonseca et al. (2014) suggested that evaluating data weaknesses through such methods might help in minimizing risks. Thus, focusing on existing security systems, including the application of injection of realistic vulnerabilities may lead to better system security.

Additionally**,** database managers play a significant role in securing database systems and in helping organizational leaders reach their business objectives (Abdul et al., 2014). Such managers need technical strategies to protect organizational databases, including taking proactive measures to minimize potential attacks by cybercriminals that could paralyze the system's infrastructure. Almost every business, be it education, financial services, or healthcare industry, are controlled and managed by database systems (Abdul et al., 2014). As the amount of data created daily, such as patient information, business, or operational data grows at an exponential level, organizations need qualified database managers not only to manage the astronomical data but at the

same time to protect it from security a breach. While different establishments look for technical skills when they hire database managers, such establishments need to combine technical skills with strategies, programs, and education so that database managers can effectively minimize the rate of data breaches amongst healthcare industries.

Summary and Transition

The integrated system theory of information security management by Hong et al. (2003) provided a framework for developing the conceptual model for the research. The approach offered a productive information security strategy, procedures, and methods for researchers in understanding information security regarding different system vulnerabilities that could lead to data breaches. The literature offered valuable insight regarding security threats, risks, and challenges various applications face within the database system. The research provided valuable insights into the security threats that might lead to data breaches. Weaknesses within the database could generate severe application defects making it easier for attackers and cybercriminals to penetrate information systems. Application flaws could cause remarkable damage to systems assurance. It is imperative database managers assess system faults and evaluate how such deficiencies might lead to data breaches. Furthermore, risk analysis is an essential aspect of security. By identifying, categorizing, and exposing system risks, database managers might make appropriate fixes, including initiating and implementing appropriate measures.

Section 1 provided a list of operational definitions to give readers the precise meaning of terms. I also included assumptions, limitations, delimitations, and significance of the study to contribute to the implications of social change.

Section 2 described the details of how the investigator conducted the research. Discussion topics included purpose statement, role of the researcher, participants, research method and design, research method, research design, population and sampling, ethical research, data collection instruments, data collection techniques, data organization techniques, data analysis, reliability and validity, including internal validity, and external validity.

Section 3 includes a discussion of the findings, the application to professional practice, and the implication for social change. The chapter concludes with a recommendation for further study and personal reflection on the doctoral journey.

Section 2: The Project

Purpose Statement

The purpose of this qualitative multiple case study was to explore technical strategies database managers in Southeast/North Texas used to protect database systems from data breaches in two healthcare organizations. The findings from the study may increase understanding of the complex nature of information security practice regarding internal and external threats. The implications of positive social change include the potential for decreasing the theft of confidential or sensitive data. Implementing data breach strategies in healthcare institutions may help database managers minimize the breach or loss of personally identifiable information.

Role of the Researcher

I was the primary data collection instrument for this study. As the primary instrument for data collection in the study, I recruited participants, conducted interviews, reviewed organizational documents, engaged participants in member checking, analyzed collected data, and interpreted the study findings, including reporting results. Another part of my role was to identify and address forms of bias that might influence the outcome of the study. Thus, I outlined research limitations, assumptions, the boundary, and scope of the study, including addressing forms of bias to support the objective of the study and research question.

Additionally, it is important that qualitative researchers display skill and comprehensiveness when it comes to data analysis and interpretation (Leedy & Ormrod, 2015). I used open-ended questions to elicit sufficient detail in the responses, which led

to open discussion and follow-up questions based on the responses. As part of my role as the researcher, I took notes, recorded the interview, and made observations during the interview process. Data collection was informed by my understanding of the study topic, though currently I do not provide direct cybersecurity expertise to any organization. I have over 10 years of experience in delivering and monitoring various computer security systems and safeguarding such systems from theft, including disruption or misdirection of services. Additionally, one of the study sites is an organization where I work as an employee. Though this could have introduced bias, I do not work in the same department as the participants and have no personal work relationship with any of the participants.

I also adhered to the Belmont Report protocol regarding ethical principles and guidelines and paid attention to informed consent, assessment of risks and benefits, including the selection of human subjects. I created a safe environment for participants, which complies with the respect of human persons outlined in the Belmont Report (U.S. Department of Health and Human Services, 1979). Respect for persons involves recognition of the personal dignity and autonomy of individuals and the protection of potential participants. The report also includes the principle of beneficence, which entails an obligation to protect participants from harm by minimizing possible risks of damage, and justice, which requires the fair distribution of benefits and burdens of research.

I used an interview protocol with all the participants as a procedural guide to address the purpose of the study. I also took adequate safeguards to mitigate bias. For instance, researchers should not attempt to affect the results of the study to achieve a particular outcome (Leedy & Ormrod, 2015). Researchers injecting themselves in the

research can cause biased results (Sonuga, 2017). To mitigate bias, I was cautious about outside influence and was open to learning from research participants, which involved identifying my preferences such as failure to accept criticism.

Participants

The participants were sampled based on their skill, age, and experience. The study was limited to participants who are database managers, who are at least 21 years of age, and who have at least 3 years of IT experience. Database managers included individuals who manage database systems and maintain patients, employees, vendors, including other organizational datasets. The criteria I used for the selection of participants included (a) successful implementation of technical strategies used to protect database systems from data breaches, (b) database managers charged with protecting healthcare organizational database systems, and (c) located in Southeast/North Texas.

An extensive screening of candidates can ensure a fit for a multiple case study (Yin, 2016). Participants were selected based on their accomplishments in implementing technical strategies used to protect database systems from system breaches. To ensure participants satisfied the eligibility criteria for the study, I contacted the executive leadership of two healthcare organizations operating within Southeast/North Texas. I explained the purpose of the study to obtain their consent to participate in the study. I sent my proposal summary through e-mail for additional information regarding the research and requested they provide the initial contact details of managers in their organizations. I identified potential participants from the list provided by the executive management of these two healthcare organizations. I then sent letters of invitation to

potential participants through the e-mail specifying the goals of the study, including the consent form. Interviews containing open-ended questions were used to gather data, including organizational document review.

To gain access to research participants, I engaged the two healthcare organizational leaders to grant permission to use their facilities for the research, including engaging their employees in the research study. Engaging and establishing contacts with participants, including gaining permission to conduct qualitative research, can be a time consuming and stressful process (Monahan & Fisher, 2015). Once I received the IRB approval for data collection from Walden University, I recruited participants holding managerial positions. I e-mailed each candidate the study information requesting his or her participation in the study. Interviewers can also establish working relationships with participants by building trust; however, the interviewer must refrain from influencing the interviewee (Yin, 2016). I created a good working relationship with research participants. The association was transparent, courteous, and honest. Because potential participants were organizational leaders with the title of administrator, manager, or other associated title, I did not use identifying information for the sake of confidentiality. To guarantee privacy, all data and interview materials, including participants' e-mail addresses, were encrypted. I followed all research standards to safeguard confidentiality, including avoiding ethical violations.

Research Method and Design

The research question determined the foundation for selecting the research method and design. The qualitative multi-case method was appropriate for the

investigation because the purpose was to explore the technical strategies healthcare organizations in Southeast/North Texas use to protect database systems from data breaches. Data gathered from healthcare industries through examining organizational documents and semistructured, face-to-face interviews helped in understanding the technical strategies database managers use to protect database systems from data breaches.

Method

I used the qualitative multiple case method for the investigation. Qualitative methods are a process to collect data relevant to the meaning of the phenomenon under investigation (Hills, 2015). In qualitative studies, researchers look for a deeper understanding of human experiences and collect data relevant to the meaning attached to the objects. The qualitative research method was appropriate for the study because the aim was to examine the technical strategies database managers use to protect database systems from data breaches, which involved interpreting the lived experiences of participants.

In contrast, quantitative researchers use experimental methods, quasi-experimental designs, and nonexperimental correlational designs to examine cause-and-effect relationships among variables such as knowledge, skills, abilities, or attitudes (King, Pullmann, Lyon, Dorsey, & Lewis, 2019). Investigators using quantitative methods emphasize mathematical or numerical measurements using experiments or structured questionnaires. Quantitative methods involve the deductive and objective process of inquiry to highlight generalizable statistical findings and test hypotheses

(Boeren, 2018). The deduction approach may explain study variables and relationships through the development of hypotheses testing. Quantitative methods are more meaningful when used to compare data systematically. Such a comparison may relate to analysis between groups. Researchers typically select the quantitative approach to test theories using empirical data. However, a quantitative design was not appropriate for addressing the present research because the study did not involve testing or measuring variables.

Further, mixed methods require a combination of qualitative and quantitative methods (Venkatesh, Brown, & Bala, 2013). In mixed methods, the researcher may utilize the qualitative and quantitative techniques to incorporate findings, including drawing inferences from both the qualitative and quantitative components (Venkatesh et al., 2013). Researchers conducting mixed methods may face challenges such as integration of qualitative and quantitative data or sampling techniques (Venkatesh et al., 2013). Using mixed methods also requires knowledge of both qualitative and quantitative techniques, and there will be more than one process of data collection. Researchers engaged in mixed methods may also utilize both deductive and inductive reasoning to support research findings when using both qualitative and quantitative methods. Finally, mixed-methods is complex and may require extended time for the researcher to complete due to the manipulation of both qualitative and quantitative methodologies (Leedy & Ormrod, 2015). Mixed-methods was not appropriate because I did not combine the elements of qualitative and quantitative research methods in this study.

Research Design

The study involved a qualitative multiple case study. The multiple case study was suitable for the research to explore technical strategies database managers in Southeast/North Texas used to protect database systems from data breaches. The multiple-case design is intended to capture the richness, diversity, and intensity of an investigation from multiple viewpoints (Civitillo, Juang, Badra, & Schachner, 2019). Researchers employ case study methods when (a) the objective is to answer how and when questions, (b) the researcher cannot manipulate the behavior of participants, and (c) contextual, and boundaries are not clear between the phenomenon and the context (Yin, 2014). Studies with a multiple case design offer an increased prospect of study replication and more persuasive findings (Marshall & Rossman, 2016). The multiple case study is useful for investigating technical strategies database managers use to secure organizational healthcare database systems from security breaches. A case study is preferable when investigating a phenomenon due to its ability to provide researchers with different sources such as observations, documents, or interviews.

Various designs were also examined for applicability, though the case study is the most suitable for the study. For instance, the phenomenological investigation is used to understand people's perceptions or viewpoints of a specific situation such as the experiences of individuals regarding a phenomenon (Handwerker, 2018; VanScoy & Evenstad, 2015). Phenomenology involves a clear stance, whereby the investigator may seek to describe the essence of experiences (Faronbi, J. O., Faronbi, G. O., Ayamolowo, & Olaogun, 2019). The phenomenological design could have been useful if I had set out

to understand the lived experiences of participants. However, the goal of the study was to explore the technical strategies database managers use to protect database systems from data breaches and not to understand the lived experiences of participants.

I also did not employ the ethnographic method. Ethnography involves understanding the cultural behaviors of participants (Baskerville & Myers, 2015). Ethnography suggests the researcher immersing him or herself within the settings of the cultural group understudy to grasp participants' behaviors (Small, Maher, & Kerr, 2014). One of the main characteristics of ethnography is the study of groups and communities seeking to observe practices, culture, ideologies, or language that is shared among groups (Mol, Silva, Rocha, & Ishitani, 2017). The amount of time spent in understanding the cultural practices of participants might prolong the research process. The longer the amount of time the investigator spends on gathering materials during a research process, the more information collected on the phenomenon in question (Small et al., 2014). Because the study was not intended to gain knowledge about the cultural patterns of database managers but to explore the strategies database managers used to protect systems from security breaches, ethnography was not considered to be an appropriate design.

Finally, I did not use the narrative design for the study. A narrative design articulates the story of individuals, including requesting one or more persons to provide stories about their lives (van der Vyver & Marais, 2015). The method may be used to explore the experience of a group and how the physical, social, and cultural environment impact and shape their practices (Haydon, Browne, & van der Riet, 2018). A narrative

approach probes into peoples' experiences based on storytelling, including how they experience the world in which they live. However, the approach has moral and ethical dilemmas due to the fact it could change its stories, including frames of orientation (Lewis, 2015). The downside was counterproductive to this study's goals.

In addition to the design of the study, saturation is an essential aspect of research. The crucial element of qualitative research is to reach saturation, a point at which observing more data will not lead to the discovery of more information related to the research question (Lowe, Norris, Farris, & Babbage, 2018). Data saturation occurs when the researcher is unable to uncover any new information, coding, or themes (Fush & Ness, 2015). I acquainted myself with the interview data and triangulated participants' responses with organizational documents. After initial interviews, I engaged participants in member checking. During the process, participants either validated research analysis, clarified, or elaborated the research interpretation. Member-checking allows participants to check or approve the researcher's data interpretations, whether they are correct or meaningful from the viewpoint of participants (Iivari, 2018). Overall, member-checking aims to increase trustworthiness in research. A subsequent meeting with participants helped in increasing data saturation and improved the accuracy of the study. I completed two member-checking interviews until participants offered no new information. I reached saturation after interviewing the ninth participant.

Population and Sampling

I aligned the selection of the population with the purpose of the study. I selected the participants from two healthcare organizations in Southeast/North Texas. The

selection was focused on an estimated population size of nine database managers from the two healthcare organizations who have direct knowledge of the technical strategies used to protect database systems and would be able to provide valuable data for research.

The sampling method I used is snowball sampling. The snowball sampling method is a type of purposive sampling researchers use to choose participants who could identify other participants from the target population (Benoot, Hannes, & Bilsen, 2016). In snowball sampling, participants can identify other participants within their group (Perry et al., 2017). I identified the executive leadership of the two healthcare systems in Southeast/North Texas who provided initial contact details of database managers in their various organizations. Once I identified potential participants, I requested their assistance in identifying other participants with related goals or interests. The selection included experts in database management assigned with the responsibility of developing, coding, managing, and testing, including providing security strategies for database systems. Database managers included individuals who manage database systems and maintain patients, employees, vendors, including other organizational datasets. I sampled participants based on their skill, age, and experience, including the successful implementation of technical strategies used to protect database systems from data breaches. The study was limited to participants who are database managers and at least 21 years of age.

I evaluated potential participants and continued to recruit until I achieved the sample size. The use of snowball sampling enhanced participants in providing contact details of other potential participants (Nelson, 2016). The sampling size requires that data

collection and analysis should continue until the point at which no new codes or concepts emerge (van Rijnsoever, 2017). Snowball sampling was appropriate and assisted in meeting the objectives of the study. Data saturation determined the actual purposeful sample size. The limit of the sample population depended at the point when data saturation is reached, which represents the time when no new data and themes emerge. Qualitative research methods typically do not require a specific sample size to yield ideal research results. Instead, sample sizes for qualitative studies vary greatly depending on the particular needs and goals of the given research. While the estimation of sample size for research participants is necessary for planning, I continuously evaluated the sample size during the research process. I used the sample size as an element of an ongoing analysis, where I compared every new observation with previous analysis to identify similarities and differences. Boddy (2016) argued that the concept of data saturation is met when no further information or themes are observed in the completion of additional interviews and is useful in determining sample size in qualitative research.

Qualitative researchers collect and analyze data until they achieve data saturation (Fusch & Ness, 2015). Hancock, Amankwaa, Revell, and Mueller (2016) noted that the gold standard of qualitative research is data saturation, which occurs when the researcher does not receive additional information from participants. At that moment, saturation will happen, and there will not be any need to select other participants for further data collection. Hagaman and Wutich (2017) stressed that data saturation establishes that sufficient data has been collected for detailed data analysis. Data saturation enables the researcher to proceed with the interpretation data. The initial sample size was eight

participants, but I continued to recruit until I reached saturation. Saturation was reached after interviewing the ninth participant. By interviewing nine database managers from the two healthcare systems, I was able to obtain all information from the participants based on the interview questions and was able to reach saturation. To ensure data saturation, I proceeded with member check interviews to guarantee no new information emerged.

Ethical Research

Ethical safeguards in research involving human subjects are indispensable to protect participants. Before data collection, I obtained IRB approval from Walden University. My IRB approval number is 05-22-19-0484795. After IRB approval, I started the data collection process. I sent the consenting form via an email to the participants. The form included the details of the study, such as ethical concerns, dangers that may exist, the right to decline or withdraw from the study at any time, the voluntary nature of participation, and instructions to indicate participant's intent to participate in the study. Krajnović and Jocić (2017) stressed that informed consent includes participants' rights, details of the study, including instructions to indicate acceptance to contribute to the study. I explained the purpose of the study, the duration of the research and procedures, including the risks and benefits. While the researcher needs to explain the purpose of the study to participants, Ross, Iguchi, and Panicker (2018) underscored that the basis of ethical standards involves protecting participants from risks and harm. Ethical issues encompass responsibilities toward participants. Such duties include confidentiality. Confidentiality is crucial because it helps to build trustworthiness between the researcher

and participants. Building trustworthiness could reduce participants' concern regarding harm that could result from the research (Ke, 2016).

The ethical protection of participants is critical in research. I informed study participants they are free to act according to their wishes. I notified participants in the letter of consent they are free to withdraw from the study at any time. Withdrawing participants will inform the researcher about their change of plans through the email. The factors that may lead a participant to decide to withdraw vary from one participant to another. Nevertheless, to maintain the ethics of the Belmont Report, all participants could leave the study freely at any time. I took several measures to safeguard all ethical principles within the study. I notified potential participants through the email that I will protect their identities with codes. I identified participants as (participant 1 or 2) and their organizations as an organization (X or Y). I encrypted the codes. Participants' protection included guarantees that I will not disclose or divulge any confidential information, treat confidential information in a manner that might expose participants or institution under study, or conduct the study in a way that might expose research participants. I sought voluntary consent from all participants. While seeking voluntary consent from participants, I encouraged them to exercise their free choice and did not use force, deception, pressure, or intimidation. I stressed I would respect a participant's decision to leave the study without demanding for any reasons. I followed Walden's ethical guidelines and the Belmont Report protocol to maintain ethical standards (Marshall & Rossman, 2016).

I notified participants they would not receive any incentives or monetary benefits. In some research studies, researchers may provide financial incentives to entice participants into being part of a research process (Lee, Lim, Kim, Zo, & Ciganek, 2015). I did not use any form of incentive to bait participants to be part of the study. Some researchers argue that building trust is a more efficient way of collecting data from participants than offering rewards (Lee et al., 2015). I notified participants that their involvement in the study is voluntarily, but the information they provided during the research could offer database managers with strategies on how to minimize data breaches in healthcare industries.

The research entails respecting the rights, privacy, and integrity of institutions within which the investigation will occur. Gergen, Josselson, and Freeman (2015) elaborated that privacy requires the protection of participants' identity throughout the study process. I coded participants' names, employment positions, or organizational names to protect their integrity. Gergen et al. (2015) explained that protecting participants with codes is one of the best ways to provide added confidentiality. I safeguarded participant and organizational information in a password-protected document that is separate from the actual study data on a USB storage device that is also password protected. I stored the study data on a second password protected USB storage device and kept the USB devices and organizational paper documents in a locked cabinet in my home. I will destroy all research materials at the end of five years. To destroy the research materials, I will format electronic records and shred paper documents.

Data Collection Instruments

Data collection was one of the most crucial steps in a research study. Data collection is a methodical approach utilized by a researcher to gather information concerning ideas, concepts, and phenomena to answer research questions (Elo et al., 2014). Data collection occurs through the use of various instruments and methods to obtain information about the subject being studied.

Instruments

I was the primary data collection instrument in the qualitative multi-case study. As the primary collection instrument, I recognized my role as the primary instrument to ascertain any assumptions that might keep the research from achieving its objectivity. Haahr, Norlyk, and Hall (2014) indicated that in a qualitative inquiry, researchers must see themselves as the principal instruments in the research process. The primary tool I used for data collection was the semi-structured interviews and review of organizational documents. I utilized semi-structured interview questions to elicit information from nine participants. According to Boyacı, and Güner (2018), semi-structured interviews allow participants to reflect on personal experiences. I used open-ended questions to allow participants to share their thoughts and detailed experiences. Semi-structured interviews are efficient means of gathering data in qualitative research due to its ability to enable the investigator to design and refine methods in conducting interviews (Peters & Halcomb, 2015). By using semi-structured interviews, I focused on exploring the strategies database managers used to protect database systems from security breaches. The semi-structured interview format included open-ended and nonrestrictive questions.

Yin (2014) argued that open-ended questions afford the investigator with an appropriate instrument for gathering perspectives from participants. Open-ended questions allowed participants to evaluate the research question, including elaborating their responses. I conducted semi-structured interviews with nine participants, and each participant received eight open-ended questions. The interview adhered to procedures such as prompts to collect informed consent or reminders for research purposes. Thus, I interviewed following the interview questions identified in (Appendix A). Dikko (2016) contended that an interview protocol is a set of rules and guidelines for the conduct of the interviews. By enhancing the reliability of interview protocols, researchers can increase the quality of data they obtain from research interviews (Castillo-Montoya, 2016). The individual interviews were conducted at the sites of the organizations under study. The conversations were recorded with the consent of participants and transcribed right after discussions. I also took notes during the meetings so that a complete record of the discussions are available for analysis. Qualitative research often involves the collection of data through extensive interviews, note-taking, or tape recording (Renz, Carrington, & Badger, 2018). I equally collected data by reviewing organizational security policies, training, and education manuals, access controls, including the use of internet and electronic mail. I reviewed organizational documents to collect additional data. The review assisted in carrying out content analysis to identify core elements and recurring themes and patterns relevant to the strategies database managers used to protect database systems from data breaches. The review of the corporate document was vital in understanding practices and standards; the two healthcare organizations in

Southeast/North Texas employed to safeguard the database infrastructure against potential breaches initiated by cybercriminals.

Once I completed the initial face-to-face interview and review of organizational documents, I performed member checking. Member checking occurs when the researcher offers research findings for participants in scrutinizing and validating (Iivari, 2018). The participants and I completed another interview of member checking. In the follow-up interview, I shared a concise summary of participants' responses from the original open-ended questions and allowed participants to respond. It is up to participants to either correct, validate, or expand my interpretations. I also checked and clarified with participants any unclear terms or verbiage that might hinder the accuracy of data interpretation. I equally scheduled another member checking with participants to go over research interpretations and summaries I discovered from the first and subsequent interviews for accurate validation. Birt, Walter, Scott, Cavers, and Campbell (2016) suggested that member checking allows participants to check, edit, clarify, and approve the accuracy of the information they provided. Member checking enhances the trustworthiness of results, which is the bedrock of high-quality qualitative research and helps explore the credibility of results (Birt et al., 2016). Data triangulation occurred through member checking to ensure accuracy during data analysis (Bacon, Lam, Eppelheimer, Kasamatsu, & Nottingham, 2017). Through member checking, the participants corrected, validated, and confirmed that my understanding and interpretation of their interview responses are correct. Such assurance improves the reliability of qualitative research and is central to establishing validity.

Data Collection Technique

The data collection technique for the qualitative multiple case study involved the use of face-to-face interviews, including document reviews, to gain a deeper understanding of experiences through interaction with participants. Clark and Vealé (2017) stated that the researcher is the main instrument in the process of data collection. As the main instrument in the data collection process, I paid attention to any assumptions that could prevent me from achieving objectivity in the study. Before data collection, I sent out letters of invitation to participating organizations. Once I received the letter of cooperation from the executive leadership from the two healthcare organizations under investigation, I requested their help in obtaining the email addresses of potential participants. Once I got the email addresses, I sent out the consent. The consent form explained the purpose of the study to allow participants to decide whether or not to participate in the study. Consenting participants chose the venue and time of face-to-face interviews. Before the meeting, I contacted each participant to ensure their availability for the interview. The interview was conducted in a reserved room to ensure privacy. It is essential to build rapport with interviewees. Before the actual meeting, I explained the purpose of the investigation and read the consent form to the participants to make sure they understood the purpose of the study. I assured them of confidentiality, including the interview will not go beyond 1hr. I obtained permission from each participant to record or take notes during the interview. Each participant received eight questions. During the interview, I paid attention to verbal, physical, and non-verbal behavior in the natural setting and used note-taking as a second instrument to understand participants'

worldview. While the interviewee was responding to questions, I took notes and made sure it did not disrupt the process. At times if the interviewee gives a short answer, I encouraged the interviewee to expand or elaborate his/her responses to the question.

To conclude the interview, participants had the opportunity to share any additional information, recommendations, or solutions to the problem. Peters and Holcomb (2015) asserted that researchers use face-to-face interviews to understand the world around them from the subjects' point of view, including unfolding the meaning of peoples' experiences. Zhang, Kuchinke, Woud, Velten, and Margraf (2017) highlighted that through face-to-face interviews; researchers could gather more knowledge from the participants' point of view. After I completed each interview, I reviewed the notes I had taken along with the recording. This process allowed me to transcribe the data, including addressing any information that required clarity.

I engaged participants in member checking to clarify, edit, including approving the accuracy of research findings. I used member checking to validate the correctness of information participants provided during interviews. Iivari (2018) asserted that the member checking technique helps to confirm the outcome of qualitative research. Member check gives participants the opportunity to clarify, and approve the accuracy of the information they provided during interviews. Member checking occurs when researchers return to participants to check for accuracy and resonance (Anney, 2014; Bacon et al., 2017). After the initial member checking, I scheduled another interview to conduct a follow-up interview with participants. In the follow-up interview, I shared a concise summary of my understanding with participants, including any unclear verbiage,

and allowed participants to verify research interpretation for accuracy. Birt et al. (2016) pointed out that researchers engage research participants in member checking to check, edit, and clarify research findings. Such a process is an appropriate technique for enhancing the trustworthiness of research findings.

I used the document review protocol to evaluate and understand the strategies the two healthcare organizations used to protect organizational database systems. The purpose of this protocol was to guide the collection of secondary data. I used the protocol to inform the participants about the types of documents I intended to review. I collected documents such as security policies, training, and education manuals, access controls, including the use of internet and electronic mail. Organizational documents helped identify key elements, or reoccurring themes and patterns applicable to the strategies database managers used to protect organizational database systems from data breaches. Sharing of corporate documents and present strategies for fighting data breaches helped secure additional data. Once participants approved research findings through member checking, l imported the results into the NVivo software program for data analysis.

Data Organization Techniques

The ability to create, organize, protect, and store data enhances the capability to access, manipulate, and regulate who may control and access it. Researchers employ different data organization methods such as file naming, reflective journals, or research logs to organize research data for ease tracking and management (Lasrado & Uzbeck, 2017). Having research journals available allows knowledge to be accessible and shared readily (Lasrado & Uzbeck, 2017). The reflective journals included experiences and

events that occurred during face-to-face interviews and document review. Cathro, O'Kane, and Gilbertson (2017) highlighted the need for the researcher to organize collected data such as reflective journals, themes, research logs, and labeling systems for easy accessibility. Reflective journals included personal views, opinions, feelings, or sentiments, which may influence the outcome of the study. I created folders by using unique file names in a password-protected format. Documents were labeled and categorized according to participants and organizations under investigation for easy retrieval. I encrypted research documents, including semi-structured interviews and member checking scripts with NVivo software and stored them in a Dropbox to guarantee data, will not be lost. Hard copies, such as organizational documents and notes, were stored in a locked file cabinet in my home. I organized, categorized, and labeled research documents for easy retrieval. I created a backup file using a flash drive. I encrypted the data to ensure document confidentiality. I will keep all data, including electronic and hard copies, for five years. Destruction and disposal of all materials, including hard copies, encrypted, and electronic documents, and all data stored in a dropbox will occur at the end of five years.

Data Analysis

Qualitative researchers ask open-ended questions to discover meaning within the study. Therefore, gathering, organizing, analyzing, and interpreting data is an essential task in research. I used the interview protocol and proceeded with data analysis. The analysis involved (a) compiling the data, (b) disassembling the data, (c) reassembling the data, and (d) finalizing the meaning of the data (Yin, 2014). Kerwin-Boudreau and

Butler-Kisber (2016) indicated that data analysis could be enhanced through the use of one or more analytic procedures. I used methodical triangulation for the data analysis. The advantage of the method is that with the combination of various data sources, the researcher might overcome the weaknesses that might exist in one data source (Joslin & Müller, 2016).

Methodological triangulation was the most appropriate data analysis technique to increase assurance of study validity and enhanced understanding of research findings. I achieved the interpretation relevant to the data in the analysis of interview transcripts and document review information in the multiple case study. Methodological triangulation is the utilization of various data sources to enhance the collection of comprehensive data to answer the research question (Abdalla, Oliveira, Azevedo, & Gonzalez, 2018; Hussein, 2015). Using methodological triangulation when conducting multiple case study improves data collection, including data analysis. The use of triangulation when conducting multiple-case study research improves data and ensures that data is rich in depth (Fusch & Ness, 2015). I approached the organizations under investigation to obtain documents relating to security policies, training, and education manuals, access controls, including the use of internal and electronic mail.

The data analysis method consisted of comparing and contrasting themes that emerged from the collected data. Yin (2016) argued that analyzing qualitative data involves ensuring reliability and validity in the data analysis, including providing plausible explanations from the findings. The data analysis focused on uncovering the key concepts from the raw data. The analysis involved getting a comprehensive

understanding of the data I collected. Such included a review of the interview transcript and member checking to gain a broad knowledge of the raw data. I organized the data obtained from face-to-face interviews through the use of code names, including reviewing documents by subject. After transcribing the interviews, I compared different interview responses. I tracked themes and similarities, identified and analyzed patterns, concepts, and ideas, and grouped similar responses from participants into easily understandable categories using NVivo. NVivo 12 is a qualitative data analysis computer software that reduces manual tasks and gives the researcher more time to discover themes, including conclusions (Atkins, Woods, Macklin, Paulus, & Atkins, 2016). Adewunmi, Koleoso, and Omirin (2016) used NVivo to process interview transcripts, including analyzing themes and patterns in examining benchmarking barriers among Nigerian facilities management. Organizing and analyzing ideas and concepts intended for coding resulted in identifying relevant themes, patterns, or recurring ideas.

The thematic analysis helps in the identification of themes and patterns across datasets while describing the phenomenon under investigation. The thematic analysis involves becoming familiar with raw data, generating initial codes, searching for themes, reviewing themes, defining and naming themes, including the production of the report (Billen, Madrigal, Scior, Shaw, & Strydom, 2017; Wheeler & Mcelvaney, 2018). El Said (2017) asserted that the thematic analysis technique is suitable for analyzing qualitative data. To be familiar with the collected data, I read and re-read collected data and searched for meanings and patterns until I became familiar with the dataset. Several readings of the transcripts enhanced the identification of explicit or repeating issues and patterns. Coding

was accomplished by labeling relevant words, phrases, sentences, or sections. I used coding to generate similar themes and patterns for data analysis. Yin (2014) presented methods for scrutinizing data in qualitative studies, including multiple case study designs. Yin's method involves analyzing data in a series of levels, from general to specifics. The process of analyzing semi-structured face-to-face interviews included the transcription of an interview into a text format to organize the raw data. I used a coding scheme for the analysis of raw data. The process took different iterations while I searched for data that corroborated or contradicted the research theme.

I combined relevant codes into overarching themes. Themes were defined and given names that provided a full sense of the theme and its importance. After initial coding, through the dissection of interview transcripts into distinct phrases, words, or paragraphs, I carried out axial coding. Weidmann (2015) suggested that axial coding involves linking data, classifying it, establishing the major categories and subcategories, and assigning codes to small segments of interview and document review. I analyzed organizational documents into a similar procedure, separating the information into categories and subcategories, including reassembling data to uncover themes that appear to be similar.

Additionally, the analysis of data involved the generation of reports, which included significant themes and how such themes tied to the literature review and conceptual framework. The conceptual framework that grounded the study is the integrated system theory of information security management developed Hong et al. (2003). The approach is an inclusive framework and a useful managerial measure that

could elevate organizations' security. NVivo software was a significant key in sorting out themes and subthemes in the generation of the final report, which I explored in the presentation of findings in Section 3.

Reliability and Validity

Reliability and validity is a requirement for qualitative research. Documenting data truthfully is critical to the credibility of a qualitative study (Marshall & Rossman, 2016). While reliability signifies the repeatability of research results, validity denotes the accuracy of data (Spiers, Morse, Olson, Mayan, & Barrett, 2018). According to Leung (2015), validity determines if research conclusions are appropriate to the study, while reliability relates to how valid the study's process and findings could be recreated. Reliability and validity involve four key areas (a) dependability, (b) creditability, (c) transferability, and (d) confirmability (Elo et al., 2014). Reliability and validity are essential in qualitative studies to guarantee that data is truthful and accurate.

Reliability

The purpose of reliability in qualitative research is to document detailed procedures in a way that future researchers interested in the study could replicate the findings (Cronin, 2014). Reliability is a requirement for qualitative research. Reliability denotes the correctness and accuracy of research findings in an unbiased form (Smith & Johnston, 2014). Spiers et al. (2018) highlighted that to establish reliability; the researcher must document the whole research process from the beginning to the end. To guarantee credibility, I recorded research data accurately. An accurate recording is

critical to the credibility of the research investigation. I did not engage my personal opinions in the findings of the study.

I took precautions to minimize my personal bias. According to Marshall and Rossman (2016), the procedures needed to demonstrate reliability include (a) utilizing a case study protocol, (b) recording and accurately transcribing study data, (c) documenting data analysis techniques, and (d) disclosing the procedures used in the case study. I ensured that data collection is reliable by conforming to the same protocol and questions for all participants. I employed other techniques such as member checking, methodical triangulation, including feedback from participants throughout the research process. I employed methodical triangulation, which is the use of multiple data sources to ensure the collection of comprehensive data to precisely answer the research question. The use of member checking allowed participants to review the analysis of interview responses to ensure research interpretation is accurate. Iivari (2018) indicated that researchers engage participants in the member checking process to evaluate, edit, comment, clarify, or confirm the accuracy of research findings, including providing additional information. In member checking, participants confirmed the research interpretation, which added more credibility to the research. Member checking is an appropriate technique for enhancing the trustworthiness of data collection, including the study findings in the study.

Validity

In the qualitative investigation, validity ensures the truthfulness of research findings (Pozzebon & Rodriguez, 2014). Validity relates to the overall accuracy and credibility of research findings. Validity does not necessarily question the credibility of

participants' responses to research questions; instead, it asks if the researcher's conclusions are representative of participants' ideas (FitzPatrick, 2019). Qualitative researchers use dependability, credibility, transferability, and confirmability to ensure the quality and completeness of the study results (Anney, 2014).

Dependability. Dependability relates to the stability of data over time (Elo et al., 2014). Qualitative investigators employ adequate measures to record their activities for reliability and consistency (Cronin, 2014). Listing each criterion used in the research to select participants in the study helps to achieve dependability (Elo et al., 2014). To enhance dependability, I transcribed study findings and analyzed research data. I afforded participants involved in the study the opportunity to evaluate research findings, the investigator's interpretation, including their recommendations to support the investigation. I engaged participants in the member checking process to establish the extent to which the results of the research are dependable. Member checking took place after data analysis to make sure transcribed data is accurate and dependable. Researchers engage participants in member checking to check whether the study findings and conclusions reflect the information participants shared with the researcher. I documented all research procedures and maintained a research journal, including noting different phases of data collection, as well as analysis and interpretation of data.

Credibility. Credibility is the level of accuracy and trustworthiness involved in documenting data correctly (Marshall & Rossman, 2016). To establish credibility and reinforce the veracity of the study findings, investigators use triangulation to validate the completeness and integrity of data collection instruments (Anney, 2014). Accurate

documentation is critical to the credibility of research in a qualitative study. I compared and contrasted different interpretations from research participants to identify differences and similarities between data sources, themes, and associations to the research. Methodical triangulation is a crucial part of qualitative research. I utilized methodical triangulation to obtain supporting evidence from the data collected through semistructured interviews and document review to guarantee that the collection of data from multiple sources answered the research question and in so doing, draw a concise conclusion.

Transferability. Transferability is an essential aspect of reliability in the qualitative case study. Transferability encompasses obtaining dependable results that are transferable to other settings (Marshall & Rossman, 2016). Transferability embodies the degree to which the results of the research are transferable to different contexts (Elo et al., 2014). I accurately recorded research observations, including documenting assumptions noted in the study. I explained the research methodology involved in the study, such as the selection of participants, data interpretation, including reporting of findings. Ensuring detailed reporting of research methodology could enable future investigators to determine study transferable results and probably use the results for future research. Accurate documentation of the investigation will provide transferability to other groups. Patino and Ferreira (2018) alluded that such is possible based on the fact the researcher provided enough information for other researchers to transfer findings.

Confirmability. Confirmability in qualitative research relates to whether the researcher will provide adequate information for other researchers to transfer research findings

(Barnes, 2015). According to Patino and Ferreira (2018), such refers to which degree other researchers could corroborate the interpretation of the current study results. It means that results must reflect participants' responses (Pozzebon & Rodriguez, 2014). To authenticate the quality and accuracy of research findings, I used methodical triangulation to compare and contrast research findings obtained from the analysis of face-to-face interviews and organizational document review.

Transition and Summary

The purpose of the qualitative multi-case study was to explore technical strategies database managers used to protect database systems from data breaches. The data collection involved a two-process format involving organizational document review and semi-structured interviews in a face-to-face setting. The approach I set out to use in the section was suitable for achieving the purpose of the investigation. The method enhanced the collection of data from database managers using semi-structured interviews containing open-ended questions and document reviews. The methodology assisted the investigator in discovering the strategies database managers used in protecting database systems from data breaches. In Section 3, I expand on the study by focusing on critical areas such as an overview of the research, presentation of findings, application to the professional practice, and implications for social change. Additionally, I include recommendations for action and suggestions for further study. Finally, I provide reflections and study conclusions.

Section 3: Application to Professional Practice and Implications for Change

The focus of this study was to explore technical strategies database managers in Southeast/North Texas used to protect systems from security breaches. This section includes (a) presentation of research findings, (b) application to professional practice, (c) implications for social change, (d) recommendations for action, (e) recommendations for further research, (f) reflections, and (g) summary, and study conclusions.

Overview of the Study

The study was focused on exploring the technical strategies database managers in Southeast/North Texas used to protect systems from security breaches. I conducted nine semi-structured interviews with database managers from two healthcare organizations in Southeast/North Texas and reviewed company documents. Participants were database managers or individuals charged with protecting organizational database systems. Participants are from Southeast/North Texas, were at least 21 years of age, and had worked for the investigated organizations for at least three years. The interviews took place in reserved rooms at each organizations' facility. I recorded the interviews, transcribed them, and coded the results. I used NVivo 12 software to distinguish and analyze significant themes from data sources received from participants. I triangulated the data using the interviews and organizational documents.

Presentation of the Findings

The investigation set to explore the research question, "What technical strategies do database managers in Southeast/North Texas use to protect database systems from data breaches?" I recruited nine participants from two healthcare organizations under

investigation to participate in the study. I used semi-structured interviews as well as the review of organizational documents to obtain data. Participants consented before the interview. Each participant received eight semi-structured interview questions. One woman and eight men participated in the interviews. This proportion of gender did not pose any bias because the research question and interview questions were non-gender sensitive.

I also received supporting documents from the organizations and participants. At the end of the interviews, I transcribed each interview word for word. I imported data transcriptions into NVivo12 software for analysis and coding. Using Nvivo 12 software helped to identify emergent themes. Data saturation occurred after the ninth interview. The review of corporate documents helped for triangulation and validation of information obtained during the interview process. Data triangulation helped in the identification of emergent themes. The themes include (a) focus on verifying the identity of users, (b) develop and enforce security policies (c) implement efficient encryption, (d) monitor threats posed by insiders, and (e) focus on safeguards against external threats. Additionally, one subtheme emerged derived from vulnerabilities caused by weak passwords.

For this multiple case study, I used the integrated system theory of information security management as the conceptual framework. The method is crucial in understanding information security strategy and procedures for security decision-makers, providers, and users to get a better understanding of information security regarding

different perspectives (Hong et al., 2003). The findings are illustrated in the tables in each theme's discussion, which highlight the metrics from participants and documents.

Theme 1: Focus on Verifying the Identity of Users

Focusing on verifying the identity of users was one of the themes that emerged from the interviews and supporting documents. The findings demonstrated that ascertaining the identity of users is crucial for database managers to determine who is accessing organizational database infrastructure. Database managers do this through authentication mechanisms by requiring an employee, a vendor, or contractor to provide a username, password, or another form of credential. If a user offers correct credentials, the individual is authorized to access the system. When authentication measures are enforced, the primary aim is to protect data assets from security threats. Verifying the identity of users consisted of two-factor authentication, multi-factor authentication, and education which, aligned with various components for identifying users in the literature review.

Verifying the identity of users was a theme all nine participants discussed and noted was crucial. Seven organizational documents addressed the theme. Three participants stated that the key to verify a user lies in making sure users provide certain pieces of verification measures. One participant noted that organizational security must say how system users are to be identified. When a discussion regarding standards for determining the identity of users arose, all nine participants identified two-factor authentication. Six participants noted that multi-factor authentication provides extra security. Five organizational documents supported these strategies by addressing the

importance of different authentication measures to make it difficult for a hacker to sabotage database assurance.

Table 1

References to Theme 1 and Subtheme

Major/Minor theme	Participants		Documents	
	Count	References	Count	References
Focus on verifying the identity of users	9	48	24	36
Implement two-factor authentication	9	23	22	21
Consider multi-factor authentication	6	14	18	15
Provide education	5	26	14	28

Establishing security strategies to verify database users is important because effective procedures prevent vulnerability issues that could lead to illegal access to private data. Three participants indicated that authenticating the identity of users is crucial for safeguarding healthcare organizational databases from security breaches. This was supported in the literature indicating that measures for authenticating users help prevent leaks and online attacks and make it difficult for cyber attackers to diminish systems assurance (Yang, Zhang, Guo, et al, 2019; Yang, Zhang, Ma, et al., 2019) as well as prevent exposure of confidential data by illegal system users (Xie & Hwang, 2019). Thus, identifying individuals attempting to access corporate databases is significant, including classifying which information they may access. All nine participants indicated that two-factor authentication, which involves a username and a password, is already in

use. Six participants also expressed that applying a multi-factor authentication will make it difficult for cyberattacks to undermine healthcare databases. The participants added that authentication approaches revolve around something a user knows, like an identification (PIN), a password, or something a user has like a badge or a fingerprint. Two participants added that even if an impersonator could provide every piece of information, it is challenging to produce what another person has like a fingerprint or badge. Further, five participants revealed that providing education is important in securing organizational databases from security breaches because cyber attackers develop new ways to attack systems daily. The participants highlighted that training could provide employees and business associates with skills for efficient authentication measures.

Seven corporate documents demonstrated support for verifying a user's identity before authorizing the individual to access the organizational database system. The documents also highlighted the need to provide system users with education, training, and programs to better safeguard systems infrastructure. One participant said that education and monitoring how users behave with corporate regulations are essential in protecting database systems. Documents equally expressed the need for database managers to implement the best security measures to identify system users, including ensuring employees, vendors, and contractors avoid weak passwords that are easy to guess. The findings show that database managers have a significant impact on implementing security strategies used to protect organizational databases from cyberattacks. In this regard, five corporate documents demonstrated that the duty of a database manager is significant in developing security procedures to overcome system vulnerabilities that might result in

poor strategies to identify system users. Thus, the results provide guidelines for preventing information manipulation or impersonation. A reliable authentication measure could protect corporate assets from a diverse set of threats, including human error and mechanical failures.

Prior literature also demonstrated that using comprehensive security measures to verify a user before admitting the individual into organizational database systems has a significant impact on drawing a roadmap of information security. For example, Hong et al. (2003) found that inclusive security measures could diminish the security threats posed by cybercriminals, which is consistent with the findings of this study. Participants highlighted that database users must be verified through multiple security measures before permitting such individuals to access organizational databases. One participant explained that when developing authentication measures, database managers must be proactive in predicting malicious intents of cybercriminals. Another participant stated that hackers will always find new ways to exploit corporate systems even with comprehensive security measures in place. Additionally, six organizational documents highlighted the importance of implementing different authenticating measures to prevent illegal access by unlawful users. Accordingly, authenticating rightful system users plays an essential role in defining who may access a corporate database (Yang et al., 2016).

Prior literature also revealed that identifying users before authorizing such individuals into organizational database systems has a significant impact on protecting systems from illegal activities. For example, Sampemane (2015) detailed that unlawful activities could be unauthorized system modification or unethical use of a password by

individuals not authorized to access systems infrastructure. Cavusoglu et al. (2015) added that security procedures and awareness programs could prevent security violations that may result due to employee negligence or actions that stem from malicious activities. However, although security measures for authenticating users' identities protect data privacy, monitoring such systems help in identifying vulnerabilities and hazards that could lead to password leakage (Mitchell, 2015). Thus, monitoring and education are essential in defining authentication measures (Cavusoglu et al., 2015; Mitchell, 2015). This is consistent with the findings, as three participants indicated that proper authentication has a critical impact regarding who logs into the organizational database. The participants insisted such measures need to be matched with education and monitoring. Supporting documents such as security policies, technical safeguards, system audits, security vulnerability scans, and operating access controls also stressed the importance of education and tracking as the key to safeguarding information systems.

Current literature also suggests that authentication measures are critical to protecting database systems. Wang, D., Li, and Wang, P. (2018) discussed implementing a two-factor authentication method to provide access to the network. Two-factor authentication can combat security issues in wireless sensor networks, controlling what a person may access (Galdi, Nappi, Dugelay, & Yong, 2018). For example, a person will not be able to get into a secured factory if the individual has no entry code. The participants echoed these findings. Four participants mentioned that using two-factor authentication is vital to neutralize the activities of cybercriminals. According to three participants, current authentication involves a user name and password. Participants

stated that the key to having a reliable authentication measure is being able to confirm who is trying to gain access to the database. Organizational documents supported the idea of focusing on authentication measures capable of protecting corporate assets from a diverse set of threats, human errors, and mechanical failures.

Data from participants and literature aligned with corporate documents. Organizational stipulations regulated that privileged employees must swipe their badge to complete authentication. Organizational documents suggested the use of comprehensive authentication. For example, documents like security policies regulating how to choose usernames, passwords, including other possession factors, recommended the use of badge as an added verification measure. Three participants also indicated that authentication should be broad. Authentication measures should be comprehensive to protect organizations from different cyberattacks, such as keylogging (Khedr, 2018). Poor authentication strategy, such as the use of simple usernames or passwords that are easy to guess, would not be able to protect organizations from keylogging assaults. Cyber attackers can easily guess usernames or passwords or even capture keystrokes through keylogging, but it is an overwhelming task to subvert a smartcard or badge since both measures could eliminate keylogging attacks. Keylogging is often installed as a piece of malware, such as a Trojan or rootkit that is used to damage devices or steal data.

Further, organizational documents supported strengthening authentication measures. Documents designed to enhance computer security such as rules and regulations regarding the use of strong passwords and security awareness training for suggested using upper and lowercase letters, including numbers and special characters, to

enhance a password. Additionally, to enhance two-factor authentication, researchers have shown using password strength to overcome guessing or brute-force attacks. Hussain, Jhanjhi, Mati-ur-Rahman, Hussain, and Islam (2019) used a systematic framework to analyze two-factor authentication, including how to counter password leakage, arguing that a verifier table is crucial to prevent password overflow. For example, if an authorized user presents a password to the authentication server, the verifier table will check for proper credentials before granting authorization access to the user. Esiner and Datta (2019) also stressed that the method is crucial for verifying authorized users. Verifying the identity of authorized users through two-factor authentication, could defend systems against impersonation attacks, man-in-the-middle, and replay attacks, including passive and active attacks (Chandrakar & Om, 2018).

Finally, the documents supported multi-factor authentication, which the participants also mentioned. Multiple authentications can be accomplished through smart cards, passwords, and other forms of biometrics to fend off authentication weaknesses (Yevseiev, Kots, Minukhin, Korol, & Kholodkova, 2017). Smartcards and biometrics like fingerprint, including usernames and passwords, are essential to protect systems (Miss, Sinha, Shrivastava, & Kumar, 2019). I found similar acknowledgments of authentication measures in the organizational documents. For example, corporate documents stated that a password must contain lower and upper letters, including numbers and special characters. Apart from username and password, employees with higher privileges must need a username, password, and a badge to access sensitive information. The policy offered a way to mitigate potential attacks from criminals who may scan the dictionary

for passwords and usernames. Four participants indicated that privileged employees must be identified through multiple authentication mechanisms such as the use of a password, username, badge, or smartcard.

Overall, data from participants regarding security culture, education, and training are consistent with prior and current literature. The cultivation of positive security culture is an effective way to promote security behavior and practices among employees in an organization (Nasir, Arshah, Hamid, & Fahmy, 2019). Four participants stressed the need for providing education, programs, and training concerning how employees, contractors, and vendors are to behave regarding corporate databases. Five documents emphasized that employees cannot click on links, websites, or open attachments that do not originate from the organization. Three participants highlighted further reasons for focusing on security culture. The participants indicated that the security culture provides knowledge as a resource. One participant stated that when proper education is provided, system users will avoid links, websites, or attachments that could introduce malware into organizational databases. Such measures could protect corporate databases and make it difficult for cyber attackers to diminish systems assurance.

The integrated system theory of information security management, which served as the conceptual framework, was also relevant in focusing on verifying the identity of users. The framework supports the findings of Theme 1, as the conceptual model addressed the importance of database managers in developing comprehensive security measures regarding preventing unauthorized system access. The framework suggests that verifying authorized system users could prevent unauthorized access or disclosure of

sensitive data (Hong et al., 2003). Participants focus on confirming the identity of system users corresponds with the constructs of the conceptual framework. Current literature reaffirms the framework. Cram et al. (2017) provided guidelines regarding how to authenticate system users and noted that identification must engage different security measures. Clear security guideline influences how employees and business associates may act regarding organizational databases (Bauer et al., 2017). Three participants noted that one of the factors for having organizational security strategies was based on its ability to provide an extra layer of protection. The protection of information systems is usually the first process in the security risk management approach (Shameli-Sendi et al., 2016). When addressing risk assessment, the intent is to utilize multiple security mechanisms to eliminate all potential security risks, including protecting information systems from illegal users (de Gusmão et al., 2016). Such is consistent with the conceptual framework. Hong et al. (2003) noted that security measures must be comprehensive and wide-ranging. Two participants stated that inadequate user verification could initiate a significant security risk. Supporting documents highlighted the danger of insufficient identification measures.

Subtheme: Vulnerabilities caused by weak password. A subtheme that emerged from data analysis is vulnerabilities caused by a weak password. An insecure password is a subtheme to authentication. A password is a key to accessing an organizational computer. A database system without a strong password could become a target for cybercriminals just like a house without a secure lock might give a free pass to the robber. Attackers could guess a password when people use familiar names like

dictionary words, house numbers, or names of relatives. With a weak password, a hacker will not only have access to a computer but the whole network connected to the database system.

Seven participants revealed that an insecure password is a critical target for cybercriminals. Xu and Han (2019) suggested that a weak password is one that could be easily subverted through brute-force attacks. The strength of a password could be tested if such a password can withstand guessing or brute-force attacks. Five participants explained that gullible employees write a username or a password on sticky notes, leaving them in the drawer, which could fall into the hands of criminals. The participants added that a resilient password must have a combination of lower and uppercase letters, numbers, and special characters. Two participants indicated the problem of a weak password is that some employees have difficulty memorizing strong passwords. The participants added that employees use words or numbers they can remember, such as names of children and pets, or car registration numbers.

Prior literature suggested that a critical thing to do to protect systems is to avoid potential vulnerabilities caused by the use of weak passwords. The proponents of an integrated system theory of information security management believed that a combination of security measures is critical to protect systems from security attacks (Hong et al., 2003). A secure password must involve a combination of letters, numbers, lower and upper keys, including special characters that are difficult to guess by an attacker. Odelu, Das, and Goswami (2016) proposed an effective dynamic group password-based on a combination of different characters. Odelu et al. (2016) found the

scheme provides users' privacy, including online and offline password guessing attacks. However, Yu, Wang, Li., et al, 2017; Yu, Wang, Song et al. (2017) revealed that the passwords for authenticating users are susceptible to shoulder-surfing attacks in which attackers could learn users' passwords. Therefore, Yu et al. (2017) suggested changing passwords periodically to make previous passwords useless. Such is consistent with the findings. Three participants stated that implementing an appropriate password policy is crucial in overcoming brute-force attacks. The participants highlighted that a password must contain a capital, lower case, number, and special character. According to two participants, a dependable password requires the integration of different password measures. Organizational documents relating to enforcing password history, age, complexity requirements, and length, including password reset suggested using numbers, upper and lower-case letters, and special characters for a password. The document suggested encrypting such passwords.

Current literature reiterated that a password must combine letters, numbers, and special characters. Guo and Zhang (2018) conducted a study regarding the strength of a password. Guo and Zhang (2018) argued that a weak password is a threat to databases and could bring organizations to their knees if they get hacked. However, Xu and Han (2019) noted that vulnerabilities with authentication are the result of poor perception of password strength. From participants' responses, I found that database managers overlooked the need to explore practical solutions that could validate the strength of a password. Galdi, Nappi, Dugelay, and Yong Yu (2018) highlighted that the use of a weak password could create an opportunity for cybercriminals to sabotage organizational

database systems resulting in data breaches. Database managers must be meticulous in developing strong passwords that are hard to crack and ensure the security measures in place are comprehensive to safeguard sensitive information. Three participants highlighted that keeping a password for ninety days sounds pretty long and stated that security professionals suggest changing passwords every 30, 60, or 90 days. IT policy recommends changing passwords regularly. One participant highlighted the danger with regular change of passwords is that employees may end up having too many passwords and probably run out of strong passwords. The participant added that when employees change the password too often, they might skirt the rules so they could do their job with minimal disruption.

However, researchers suggested the use of symmetric encryption could protect passwords from attacks (Choi, Jeong, Woo, Kang, & Hur, 2018; Álvarez, Andrade, & Zamora, 2018). While encryption schemes could secure systems against cyberattack activities, the existing literature emphasized the role of data managers in implementing security measures to enable employees to make the right choice when selecting passwords. When employees are not guided, a wrong decision could result as a consequence. Furnell, Khern-am-nuai, Esmael, Yang, and Li (2018) conducted a study regarding variations in password meter usage and how feedback can positively affect the resulting password choices. Furnell et al. established that the difference between passwords selected by unguided users and those receiving guidance is clear. Furnell et al. (2018) claimed the study revealed a 30% drop in weak password choices. Furnell et al. added that strong passwords are one of the essential methods of user authentication.

Participant's responses align with the literature. For example, four participants highlighted that the primary goal of avoiding a weak password is to mitigate risk. The information obtained from organizational documents provided guidelines for employees when they create passwords. Understanding the benefits of avoiding an insecure password could protect healthcare organizations from security breaches.

The integrated system theory of information security management, which served as the conceptual framework, was relevant in evaluating vulnerabilities caused by weak passwords and provided the measures for addressing such weaknesses. The conceptual framework discussed the findings in the sub-theme as it highlighted wide-ranging security measures to overcome system vulnerabilities. Participants' emphasis on enforcing a strong password to surmount the assaults of cybercriminals who use guessing or brute-force attacks to diminish passwords measures aligns with the constructs of the conceptual framework. Guo and Zhang (2018) advocated for the use of a strong password and insisted that a combination of different password measures may increase the password strength. Consequently, Xu and Han (2019) discussed methods for preventing the use of weak authentication and argued that a strong password must contain all the necessary elements involving the combination of letters, numbers, and special characters. Database managers must enforce strong password policies and make sure employees comply with organizational policies. Having appropriate password measures in place could avert the use of a weak password and in so doing, save healthcare organizations from the embarrassment of security breaches.

Theme 2: Develop and Enforce Security Policies

The second theme to emerge was developing and enforcing security policies. Identifying potential risks is an essential factor when developing security policies. Security guidelines must reflect organizational goals and business objectives. Three participants highlighted that policies ought to be flawless, easy to understand, straightforward, and written in simple language employees, contractors, vendors, and business associates could understand. When security policies are developed, the goal is to protect corporate database systems from internal or external threats. Policies may specify how a username or password may be structured, including what systems may be connected to the network as well as what information users may access. Developing and enforcing security policies was a theme all nine participants discussed and noted was crucial. Seven organizational documents referred to the theme (see Table 2 for theme metrics). Developing and enforcing security policies is vital because effective security policies address constraints, rules, and procedures for all individuals accessing organizational databases.

Table 2

References to Theme 1

Major theme	Participants		Documents	
	Count	References	Count	References
Develop and enforce security policies	9	35	29	41
Implement routine audits	9	22	13	14
Monitor employee violations	6	14	24	23
Provide education/programs	5	21	22	18
Address the use of BYOD	5	9	12	10

A security policy must identify organizational assets, including potential threats to such infrastructures. Without enforcement, security policies are worthless. All nine participants noted that security policies are essential for organizations to realize their business goals and strategic objectives. Four participants stated that security policies are crucial because, without it, there is no way to define how employee behavior could lead to security threats. According to Cram et al. (2017), organizational security policies must specify how employees and users of information resources need to behave to prevent, detect, and respond to security incidents. Two participants stated that when attempting to develop security policies: "The first thing that runs through our mind is how to take proactive measures against potential threats." The participants added that policies change over time due to new cyber threats that develop daily. While deliberating how much knowledge employees, contractors, or business associates should have regarding corporate policies, seven participants noted that security policy must provide adequate education, so employees are aware of the implications of not following security guidelines. The participants highlighted that enforcement is the primary key to organizational security policies. The participants added that security enforcement might include suspension or termination of employees who flout corporate rules such as opening attachments or clicking on funny links that could contain viruses.

Five organizational documents noted that policy enforcement changes how database users behave. While reviewing corporate documents, I found that participants worked with the executive leadership to develop security policies. Three organizational records expressed the importance of being aware of new system threats. The document

added that security policies must define procedures and strategies regarding how to recover in case of a data breach. While participants agreed that security policies are crucial to protect organizational data, four participants noted that getting employees understand the importance of corporate guidelines is not an easy task. A discussion arose regarding what database managers could do to monitor the activities of employees who deviate from corporate policies? Two participants suggested the use of system audits to monitor employee habits in the use of organizational computer infrastructure. The participants' reiterated the importance of taking disciplinary actions against non-compliant employees who violate corporate policies. Six corporate documents echoed punitive sanctions, including termination or prosecution.

Prior literature demonstrated that planning information security requirements, including drafting security guidelines, is crucial in meeting organizational goals. Hong et al. (2003), outlined that while drafting security guidelines are central, users' compliance is critical for protecting data throughout its lifecycle. Researchers have argued that user's compliance is imperative for organizations to advance their business objectives. Cram et al. (2017) alluded that compliance plays a vital role in mitigating security risks. However, non-compliance could involve inappropriate employee behavior, such as opening unknown emails or downloading infected files. Such is consistent with my study findings as four participants indicated that getting employees to comply with policy procedures is not easy. Documents expressed that different strategies are used to get employees to comply with security guidelines. Documents indicated that employees and business

associates receive routine training, education, and programs regarding how to comply with organizational policies.

Participants' responses are consistent with the existing literature regarding employee compliance with organizational policies. All participants underscored the importance of security policies. Chen et al. (2018) indicated that having a clear organizational policy and motivating employees to comply is essential in realizing corporate business objectives. Consequently, without compliance, policies are useless. Two participants stated that for policies to be useful, database managers must get system users on board. Sharma and Warkentin (2018) reported that employees represent a significant threat to organizational security policies. Having a plan in place does not guarantee information security if employee compliance cannot be guaranteed (Chua, Wong, Low, & Chang, 2018). Such is consistent with the findings from participants, which demonstrate that policies rely on compliance. Organizational documents such as guidelines regarding the opening of emails and attachments not originating from the organization, clicking on external links or websites that might contain viruses, as well as unauthorized updates, reiterated the importance of compliance with corporate policies to mitigate threats or network attacks.

I found in my review of current literature that adherence to security policies is the key to advancing organizational business strategies. Sharma and Warkentin (2018) presented a study regarding how system users adhere to organizational policies and underlined that security policies must outline rules regarding how employees should access corporate information resources. Two participants stated that failure to comply

with corporate guidelines could leave healthcare organizations vulnerable to security attacks. Database managers must develop security mechanisms to monitor and confront employee violations. Continuous security event monitoring to detect suspicious behavior or unauthorized system changes, including audits was a guideline I found during organizational document analysis. The standard guided the organization on reviewing, enforcing, and implementing strategies that provide awareness of threats and vulnerabilities. The policy spelled out responsible use of organizational computers. It restricts employees, vendors, and contractors from opening emails, attachments, links, or websites from unknown sources. The policy restricts employees from playing video games on organizational computers or sharing passwords or usernames with co-workers. It relied on providing education, training, and programs for employees, volunteers, contractors, and vendors regarding the responsible use of organizational databases. Strong policies combine strategies to secure healthcare database systems.

Consequently, researchers have suggested that cyber attackers target people more than systems. Sohrabi Safa et al. (2016) presented a study on how hackers may target people instead of computers. Since organizations are making it more difficult for cybercriminals to undermine security assurance by providing extra security, hackers are targeting people more than computers. When addressing organizational deterrence measures, the first step is to provide adequate security, including making sure employees comply with corporate guidelines (Rajab & Eydgahi, 2019). Incidents involving security breaches brought about by employee negligence could ruin a corporate reputation, including costing millions in losses. Two participants acknowledged that social engineers

target people more than systems. Chua et al. (2018) suggested providing education, including monitoring employees due to their limited knowledge, is crucial for protecting systems. Four organizational documents highlighted that education is imperative to create awareness regarding new ways cybercriminals target people rather than systems.

Five participants brought up the issue of Bring Your Own Device (BYOD) and highlighted there should be a clear policy on the use of BYOD. The policy can help an organization in its daily business. However, Hovav and Putri (2016) highlighted that BYOD could be dangerous to organizations since mobile devices could carry malware and could trigger security when connected to the corporate network. The participants stressed that if the organizational policy allows employees, vendors, and contractors to use their own devices to access organizational resources, such usage could lead to data breaches. The participants added that database managers need to restrict how much information users of BYOD may access. Such is in agreement with the findings of Hovav and Putri (2016). The authors performed a study on the use of BYOD and detailed that BYOD could introduce vulnerabilities or malware into healthcare databases since such devices may not have a sufficient level of security. Enforcing security policies is critical to patient privacy, achieving corporate business objectives, including complying with the Health Insurance Portability and Accountability Act. Four organizational documents highlighted that users of BYOD, such as associates, contractors, consultants, or vendors, are prohibited from storing electronically protected health information on portable or remote devices that are not controlled, monitored, or encrypted. Security policies should

include plans, rules, and practices that regulate how an individual may access organizational database systems.

The integrated system theory of information security management was relevant to the development of organizational security policies. The method spelled out comprehensive methods organizations could utilize to develop security policies not only to advance business objectives but to discuss various ways that could lead to security breaches. Participants focus on implementing security policies necessary to address system vulnerabilities corresponds with the constructs of the conceptual framework. Current literature reaffirms the framework. Rajab and Eydgahi (2019) stressed the need to have an inclusive security policy, including proactive measures to combat system weaknesses and vulnerabilities. When addressing systems vulnerabilities, the first line of action is to implement inclusive security measures. Moody, Siponen, and Pahnila (2018) acknowledged that security policy should define how users of information and technology resources may act to prevent, detect, and respond to security incidents. This is consistent with the findings of Hong et al. (2003), who argued that a security plan should be cohesive and comprehensive to address potential vulnerabilities. Two participants stated that a unified security plan must engage different safety measures and focus on planning information security requirements. From organizational documents relating to divulging confidential information to unknown entities, sharing of passwords with colleagues, or engaging in unlawful updates, I observed that security policies covered crucial strategies in the framework; for example, procedures to educate users and

responsibilities to ensure data safety. The findings indicated that organizational security policies are critical in protecting corporate database systems.

Theme 3: Implement Efficient Encryption

Another theme that emerged during data analysis was implementing efficient encryption. Encrypting sensitive data is critical in averting a data breach. Encryption methods provide various approaches to encode messages so that only authorized individuals can access it. In encryption procedures, the intended message regarded as plaintext is encoded through the use of encryption algorithm - a cipher to generate a ciphertext that can only be read when decrypted. All participants advocated for secure encryption, and three organizational documents addressed the theme. (see Table 3 for a list of Theme metrics). Implementing encryption strategies to protect corporate data is crucial because effective encryption would deny a cybercriminal the ability to access private data. Nine participants reported that efficient encryption is critical for safeguarding database systems. Thomchick and San Nicolas-Rocca (2018) highlighted the significance of encryption and noted the mechanism is paramount for denying criminals access to private data. Participants reported that well-organized encryption keeps sensitive information confidential while in transit. While discussing the differences between weak and robust encryption, three participants stated that weak encryption is subject to interception by unauthorized entities. Two participants discussed common security vulnerabilities within databases, pointing out that a recurrent habit among cybercriminals is to look for a weak encryption algorithm. Three participants noted that storing a credit card or other confidential information in a browser is a bad idea. One

participant highlighted that imprudent computer usage by employees and vendors could make it possible for hackers to gain unauthorized access. Implementing secure encryption is imperative for protecting database systems.

Table 3

References to Theme 3

Major theme	Participants		Documents	
	Count	References	Count	References
Implement efficient encryption	9	34	18	37
Address weak encryption	9	28	24	20
Symmetric encryption	6	10	12	15
Asymmetric encryption	5	8	11	18

A significant concern when developing security strategies is to consider which feature would offer better protection. Two participants stated that encryption is crucial to protect data privacy. Zhou, Chen, Zhang, Su, and Anthony James (2019) indicated that encryption guaranteed data privacy and noted that even if an adversary intercepts data, the individual will not be able to read it. Three organizational documents underlined the need for implementing encryption mechanisms to deny unintended entities access from sensitive data. For example, documents stated that patient information or any other sensitive data such as password, data in flight, data at rest, and electronic health records must be encrypted. The findings demonstrate that the role of a database manager is crucial in developing robust encryption mechanisms.

Prior literature echoed the need for secure encryption and noted that encryption with insufficient key length could become a target for cyber attackers. An important

security decision when deploying encryption measures is to ensure that sensitive data is secure during transfer. Without appropriate deployment mechanisms, incorrect deployment of encryption schemes could lead to broken authentication, key leakage, or result in the exposure of sensitive data. However, Dai et al. (2016), indicated that several researchers investigated how different forms of encryption could protect data in transit or data at rest. Dai et al. argued that symmetric encryption, unlike traditional encryption, is based on the assumption that the data owner holds a secret key that is unknown to the adversary. In symmetric encryption, the entities communicating must exchange the keys so that it could be used in the decryption process. Two participants stated that symmetric encryption provides an extra layer of support. Organizational documents did not specifically talk about symmetric encryption but expressed that sensitive data must be encrypted through encryption mechanisms. The approach may be important in protecting database systems because the measure can guarantee data privacy, prevent illegal interception of files by cybercriminals, including protecting systems infrastructure from data breaches.

Current literature aligned with previous research and demonstrated that encryption provides robust data security, including protecting organizations from the disclosure or leakage of private data. Thomchick and San Nicolas-Rocca (2018) performed a systematic review of literature relating to encryption and concluded the measure keeps sensitive information confidential while in transit or at rest and prevents it from being intercepted by cybercriminals. Martins, Sousa, and Mariano (2017) added that in many encryption measures, homomorphic encryption is used to secure data during

transfer and protects it from disclosure, or leakage. Therefore, implementing encryption could be imperative for protecting data in transit, especially those transferred through mobile phones. Four organizational documents determined that active encryption measures are necessary to protect data both in transit or storage. The document suggested encryption for every sensitive data. The policy highlighted that every confidential information must be protected through encryption. It indicated that employees, vendors, or contractors might not use mobile devices to transmit confidential information unless such tools are secured by organizational security measures. Five participants suggested encryption for every sensitive data. The participants cited weaknesses in databases due to consistency issues, data leaks, including deployment failures. The document and participants' responses are in line with the findings. Zhou et al. (2019) explained that the encryption mechanism aims at keeping sensitive information confidential while it is being transmitted or stored to prevent interception by unauthorized entities. Zhou et al. (2019) conclusions concurred with the strategies used by participants and supporting documents for the deployment of encryption measures.

Participants stressed that encryption procedures must meet organizational security guidelines. While all participants believed that secure encryption is a significant weapon to fight security breaches, when asked which encryption model was more effective, three participants stated that symmetric encryption is relevant in protecting data. Participants' responses aligned with the findings of Baykara, Das and Tuna (2017). Baykara et al. performed a systematic study on symmetric encryption. Baykara et al. found that symmetric encryption guarantees data privacy, including deterring illegal data accesses.

The mechanism could provide stronger security measures, including offering reliable protection for data. The procedure plays a vital role in security assurance since it can guarantee a system with not only confidentiality, but authentication, integrity, and non-repudiation.

Furthermore, symmetric encryption is one of the essential techniques in cloud computing, and unlike traditional encryption, symmetric encryption is based on the assumption that the data owner holds a secret key that is unknown to the adversary (Dai et al., 2016). The approach may be crucial in protecting database systems because the measure could guarantee data privacy, prevent illegal interception of files by cybercriminals, including protecting systems infrastructure from data breaches. However, while symmetric encryption could protect data from a security breach, the significant issue with the method is that two or more parties may have access to the secret key. Furthermore, the technique could be susceptible to plaintext attacks.

Integrated system theory of information security management provided a critical element for the development of encryption but did not fully frame the findings in Theme 3, as the conceptual framework does not specifically address which types of encryption within the constructs of inclusive security measures. An extension of the framework by Tsung-Han et al. (2016), added specific constructs regarding encryption. Participants focused on the central point of implementing encryption measures necessary to address system vulnerabilities, including protecting data in flight or at rest. Participants' responses correspond with the constructs of the conceptual framework. Current literature reaffirms the framework. Baykara et al. (2017) demonstrated the mechanism plays a vital

role in security assurance. Secure encryption involves comprehensive guidelines and measures used to protect organizational data throughout its lifecycle. Such strategies include actions geared towards the prevention of interception of confidential data by unauthorized individuals except for parties who possess the secret key. A vital security measure when using encryption is to prevent the interception of confidential information. Encryption can protect patient information, emails, and other sensitive information. The mechanism could be used to protect classified information. From organizational documents, I observed that encryption strategies covered crucial strategies in the framework; for example, procedures to educate users and responsibilities to ensure data safety. The findings indicated that encryption procedures are critical in protecting corporate database systems.

Theme 4: Monitor Threats Posed by Insiders

The fourth theme to emerge was the importance of monitoring the threats posed by insiders. Insiders are healthcare employees, vendors, and contractors, including business associates and volunteers. Organizations depend on insiders to realize their strategic goals and business objectives. An insider threat may occur when an employee inadvertently or deliberately abuses organizational security policies to harm critical information systems. Monitoring insiders was a theme all nine participants indicated was important. Seven corporate documents addressed the theme (see Table 4 for theme metrics). Monitoring the threats posed by insiders aligned with various components of security strategies in the literature review. Three participants agreed that developing security procedures to monitor the activities of organizational insiders is critical because

effective strategies could prevent system vulnerabilities that might result from such activities.

Table 4

References to Theme 4

Major/minor theme	Participants		Documents	
	Count	References	Count	References
Monitor threats posed by insiders	9	32	42	40
Watch for malicious insiders	9	14	16	20
Address negligent insiders	6	30	22	25
Provide training	5	32	24	18

A crucial thing to do when considering threats posed by insiders is to monitor threat behavior. Six participants stated that insiders pose a serious threat to organizational databases and reported that an insider might accidentally open an attachment or click on a website that could contain malicious files. Ho, Kaarst, and Benbasat (2018) indicated that insiders pose a potent threat, and as such, monitoring such dangers is critical. Threat behavior may include abuse of privileged accounts, abnormal access to sensitive information, inappropriate sharing of passwords, or unusual login durations. Five participants mentioned that violations of organizational security policies are indicative of insider threats. They also stated that when policies are lacking, individuals could create vulnerabilities within healthcare databases. When a discussion regarding mischievous employees or business associates arose, five participants noted that malicious insiders intentionally break organizational security policies to steal confidential information or industry secrets. Three participants highlighted that insiders might cause damage to the

organizational databases when they choose the easy way to get their job done, thereby ignoring corporate policies. While discussing the proliferation of mobile devices like IPad, or mobile phones, three participants elaborated that such devices could introduce viruses into corporate database systems. The participants explained such systems might introduce viruses if they lack organizational security updates. Six organizational documents demonstrated the importance of monitoring illegal activities. Two documents mentioned using the audit to track unauthorized employee behavioral patterns in the use of computer resources. The findings aligned with the current literature regarding developing security strategies to monitor illegal system behavior by employees and business associates.

Prior literature demonstrated that insider threat has a significant impact on how organizations may realize their strategic goals and business objectives. For example, Jingguo et al. (2015) validated that insiders pose a substantial threat to organizational databases. According to Jingguo et al., insiders could know about internal database systems, including data security mechanisms, which makes them a serious threat. Since insiders know internal systems, deploying IDSs or auditing measures to monitor employee actions could help to minimize security breaches. Pasquale et al. (2016) found that malicious insiders have various ways to circumvent organizational security guidelines to steal or damage valuable data assets. However, Smyth (2017) noted that there is also the case of accidental insider breaches caused by employees as a result of human error. According to Smyth (2017), more than seven billion data records have been exposed and estimated that insiders were responsible for 9%. Such is consistent with the

findings as multiple participants indicated that insiders pose a severe threat to organizational data. Two participants highlighted that while insiders pose a significant threat, it is difficult to track employee negligence. Corporate documents echoed the danger posed by insiders and suggested routine monitoring for employees, contractors, and other business associates who deviate or neglect established security policies.

Ho, Kaarst, and Benbasat (2018) reiterated that insiders pose a significant threat. According to Ho et al. (2018), such risks occur when employees or vendors open emails or attachments against organizational policies. Liang et al. (2016) revealed that insiders with their knowledge and access to corporate resources could launch a more damaging attack than cyber attackers. Burns et al. (2017) echoed the finding Liang et al. (2016) regarding how insiders' knowledge could become an attack weapon against organizational systems infrastructure. Two participants stated that an employee might open a phishing or spam emails, click on an infected attachment file, or unknowingly divulge a password or username to social engineers. One participant underscored the importance of training to create an awareness regarding the danger of non-compliance with organizational policies. Organizational documents reiterated the need for providing training and programs regarding illegal activities of system users.

The findings also demonstrated, however, the danger posed by malicious insiders. Pasquale, Hanvey, Mcgloin, and Nuseibeh (2016) stated that malicious insiders could be current or former employees, contractors, or business associates who may have grudges against an organization. Since such individuals have knowledge and skills of the corporate database, they may circumvent security measures to either steal or damage

valuable organizational database systems. In short, database managers should be diligent in developing strategies to monitor employee behavioral patterns within the database network. Pasquale et al. (2016) conclusions are in alignment with participants and supporting documents regarding malicious employees who by-pass corporate policies to harm organizational databases.

Among organizational documents, I found several directives, rules, regulations, and policies geared towards monitoring insider behavior in the use of database infrastructure. Part of the strategies highlighted rules regarding the opening of emails that do not originate from corporate systems. Others detailed how attachment files have to be treated. Others included providing education on how to surmount the schemes employed by social engineers. Three participants noted that when employees or contractors lose organizational privilege either due to fraud or unethical behavior, database managers, at times, forget to cut their privilege or access to the organizational database. Such contractors might turn malicious if they still have access to the corporate network system. The findings aligned with the existing literature regarding the danger posed by insiders.

The integrated system theory of information security management, which served as the conceptual framework, provided inclusive security strategies for monitoring different types of security threats but does not fully explore the findings of Theme 4, as the conceptual model did not address various forms of insider threats. The extension of the framework by Brunisholz et al. (2015) added specific constructs into insider attacks and how such violations might encompass typical coercion schemes employed by cyber-scammers. For instance, breaches by insiders may involve making unauthorized changes

to the system database. The findings of Brunisholz et al. (2015) is consistent with the results of Ho et al. (2018), who demonstrated that unfettered insider privilege is a significant threat if not matched with security monitoring. This is also consistent with the findings from participants. Participants indicated that systems users must be audited to measure if their actions regarding database usage meet organizational security policies. Organizational documents equally highlighted the importance of reviewing how employees, contractors, vendors, and business associates adhere to corporate security guidelines.

The findings support that the participants in this study are motivated to develop different security strategies to protect organizational databases against the threats posed by insiders. The concept of using inclusive security measures such as auditing, security policies, education, and programs has a direct impact on the integrated system theory of information security management, which advocates a comprehensive security strategy (Hong et al., 2003). Therefore, database managers need to develop a comprehensive security strategy to monitor and minimize the damages that could originate from insiders.

Theme 5: Focus on Safeguards against External Threats

The fifth theme from the data analysis was the importance of focusing on safeguards against external threats. External threats could result from malicious attacks such as viruses, Trojan, worm, or spyware. Others include denial-of-service attack, eavesdropping, phishing, social engineering, including ransomware or keylogging. These types of threats are potent and originate either from a virus or social engineering schemes. For example, in a phishing attack, a cybercriminal could persuade a gullible

employee to divulge sensitive information such as passwords, usernames, or credit card information for malicious reasons. Safeguards against external threats were a theme; all nine participants discussed and noted it was critical. Eight corporate documents addressed the theme (see Table 6 for source metrics). Four participants reported that attackers might use malware, spyware, Trojan horses, or worm to infect database systems and in so doing, cause serious harm to the network system. Two participants shared that social engineering and phishing attacks are frequent among healthcare organizations and that such attacks are increasingly sophisticated. Three participants stated that a successful malware could open a backdoor a cybercriminal could use to steal or violate personal privacy. Six organizational documents expressed the danger posed by external threats, including strategies to overcome such risks.

Major/minor theme	Participants		Documents	
	Count	References	Count	References
Safeguard against external threats	9	32	24	40
Address virus infection	9	22	26	20
Implement anti-virus	6	18	13	15
Monitor social engineering schemes	5	16	11	18
Provide education				

One participant indicated that an essential thing to do when it comes to safeguarding external threats is to identify threats, assess defensive strategies, including implementing security strategies to mitigate the risk that may result from system vulnerabilities. Three participants stated that external threats are perilous to organizational database systems. Makridis and Dean (2018) highlighted that external

threats are malicious campaigns in which foreign actors exploit security exposures to attack systems. In external attacks, cyber attackers could use keylogging to capture keystrokes and use such knowledge to access private information. One participant stated that criminals could utilize standardized query language injection attacks to execute a malicious payload if vulnerabilities exist within the system. The participant expanded that a successful standardized query language attack could paralyze the database network making files or applications unavailable to legitimate users. Two participants explained that malware solutions such as automatic malware scans, Malwarebytes, and domain name system based web filtering provide adequate protection from online threats. One participant highlighted that these solutions are sufficient to mitigate against malware, spyware, or Trojan horse, including other attacks that could lead to security breaches. The participants added that without suitable security solutions when malware inserts itself into the network, it could reside within the database before undermining systems assurance. Three participants shared that external threats are sophisticated and difficult to track due to the fact the methods cyber attackers use regularly change while new viruses are written every day. Five organizational documents echoed the danger posed by external threats and underscored the importance of safeguarding databases against such threats. The document, for example, suggested using IDSs to monitor such dangers.

Prior literature demonstrated that external threats such as malware are one of the most potent threats facing organizational databases. Safeguarding such systems is a top priority for database managers. Lee and Kwak (2016) noted that hackers, including cybercriminals, develop new malware or Trojan daily, and such developments make it

difficult to find the right tools to fight such dangers. Cybercriminals seem to be ahead of security developers and have new ways to disguise viruses to compromise databases irrespective of defensive mechanisms. Kim et al. (2015) explained that in a fake antivirus, criminals could hide malware as legitimate software to convince users into installing it. Attacker's intent could be to steal or cause enormous damage to organizational businesses.

However, detecting hardware Trojans is difficult due to the fact the method used to insert them is numerous (Wu et al., 2016). Current literature demonstrated that external threats such as malware are difficult to track. Gandotra, Bansal, and Sofat (2017) argued that ubiquitous computing devices with network capabilities had become a critical target for cyber attackers. The majority of attacks are launched on system infrastructures for financial profits. The evolution of interconnected networks, the explosion of mobile devices, and cloud computing have given opportunities to attackers for discovering vulnerabilities and exploiting these for creating sophisticated attacks. Gandotra et al. (2017) highlighted that malware is one of the most dreadful security threats and argued it has the capability to circumvent the earlier developed methods of detection. Such attacks are evolving and making use of new ways to target computers and mobile devices. Besides, the intensification in their volume and complexity has increased the damage caused by such attacks. Two participants stated that databases must be built to prevent unauthorized or intended activity. The participants added that design flaws and programming bugs could create system vulnerabilities, which could lead to data loss or corruption caused by the entry of invalid data or performance degradation. Three

participants indicated that in software development, care must be taken to surmount challenges such as insufficient software metrics, inappropriate testing tools, or coding language could create technical problems that could lead to data breaches. The participants stressed that solutions such as packet filtering are imperative to protecting databases from security attacks. The participants noted that while packet filtering blocks or passes packets at the network interface based on the destination address, it equally protects the local network from the intrusive packet by examining the header. Such measures are crucial by enabling the filter to either allow or prevent the packet from passing. One participant highlighted the importance of encryption. The participant stated the solution is used to enhance the security of the packet by scrambling the contents so that it can be read-only by someone who has the right encryption key to unscramble it. The measure could be used to encrypt patients' patient health information, phone number, or credit card numbers to make sure the information is secure. Organizational supporting documents backed the solutions highlighted by participants and stressed the use of packet filtering and encryption to defend against external threats. When a discussion regarding the use of audits arose, four participants stressed that system audits are crucial in preventing external attacks. The participants stated that audit management tools like Netwrix could detect security threats and shield database environments from ransomware, malicious insiders, including alerts from new threats patterns. The participants maintained that security managers could proactively use the solution to mitigate the risk of insider misuse, including identifying security gaps and inactive accounts. Two participants expanded the issue of mitigating insider threats and noted that

system audits, education, programs, and training are critical in preventing security breaches. The participants indicated that education creates awareness of how cybercriminals could hide viruses when they send emails, attachments, or web-links to launch attacks. The participants added that gullible users without appropriate training could open such emails or attachments, causing the virus to install and replicate itself against the database infrastructure, causing the system to misbehave. I found similar acknowledgment of system audits and education in the organizational documents. For example, four corporate documents stated that database managers should use audits to monitor database system, including providing regular education and training to create awareness of security threats posed by cybercriminals.

Existing literature was consistent with my study findings regarding safeguarding external threats. Makridis and Dean (2018) indicated that external threats such as the use of malware by cyber attackers against organizational system infrastructure represent one of the most significant external threats against organizations. Several kinds of malware, such as Trojans, worms, adware, or spyware, could be used to infect databases. Three participants reported that once a system is infected, confidential data might be intercepted and possibly read by intruders due to the presence of malware. According to five participants, while having antivirus programs is crucial, fighting infected databases could become an arduous task. Two participants highlighted they use firewalls, antivirus software, IDSs, including anti-spyware and employee education, to fight external threats. I equally found policies regarding employee education and programs regarding organizational behavior as well as the implementation of IDS to prevent breaches.

Education and programs could assist employees in defeating social engineering tactics, including overcoming the schemes and threats posed by such tactics.

The literature equally provided some solutions to social engineering attacks. Hatfield and Loukas (2018) conducted a study on social engineering and found that cybercriminals use deception to induce employees into divulging private information to unauthorized entities. Siadati, Nguyen, Gupta, Jakobsson, and Memon (2017) equally stated that manipulation is one of the arsenals social engineers use against naive employees into undermining privacy. Hatfield & Loukas (2018) and Siadati et al. (2017) concluded that social engineering schemes constitute a significant weapon against naïve employees. Five participants reported phishing, pointing out how gullible employees could be manipulated into divulging confidential information by social engineers. Participants' responses tallied with the literature. Organizational documents referenced social engineering attacks and highlighted education and training as one of the ways to combat such attacks.

Current countermeasures against social engineering include outsiders or insiders who perform technical vulnerability assessments or end-user oriented phishing tests. Three participants stated that creating a security culture is crucial in minimizing social engineering vulnerabilities. Organizational documents offered policies for combatting social engineering attacks. It stressed the danger against employees sharing a username, password, or using colleagues' badge to login. The policy added that funny links or websites don't usually have correct spelling and recommended employees not to click on

such links. Participants' responses regarding combating social engineering schemes corresponded with supporting documents and current literature.

The integrated system theory of information security management provides an essential element for addressing external threats. The theme appears aligned with the framework. The findings support that the participants in the study are motivated to deploy security strategies used to safeguard organizational databases from external threats. The concept of using inclusive security mechanisms to fight external threats is in alignment with ensuring data privacy. Such has a direct positive impact on the attitude of database managers towards using comprehensive security measures (Hong et al., 2003). Using inclusive security measures could minimize the anxiety database managers may feel regarding the danger of external threats. The reduction of database threats is conversely related to wide-ranging safety mechanisms designed to deter cyber attackers (Tsung-Han et al., 2016). Such is also consistent with the findings from participants, which validate the use of different security measures to protect organizational databases from external threats. Corporate documents equally stressed the importance of unified security measures.

In summary, healthcare organizations face several security breaches from external threats. Such threats may have the potentiality of causing severe harm to the database systems. Database managers have the burden to develop integrated and well-coordinated security mechanisms. Such measures could minimize several attacks orchestrated by cybercriminals. A defined security strategy could help mitigate concerns regarding data security, availability, integrity, and privacy.

Applications to Professional Practice

The challenges related to protecting database infrastructure from data breaches has increased over the years. Database managers are increasingly finding it difficult to find the best security solutions to protect systems due to the activities of cybercriminals, including system weaknesses.

Database threats are a global issue due to interconnected information systems. Healthcare organizations create so much information, and they use database systems to make their information available to intended users. Therefore, data is a critical asset, and there is a need to protect it from security threats, including implementing countermeasures to forestall threats from criminals. Unfortunately, global networking makes it difficult to protect data from the hands of malicious attackers, processes, unauthorized users, and insiders. Information Security Breaches Survey (2015) highlighted that 90% of large organizations had suffered an information security breach. Organizational employees have accounted for 59% of security incidents (Manworren et al., 2016). Consequently, unauthorized use of computers by employees accounted for $40 billion in losses (Manworren et al., 2016). As a result of unapproved use of computers by employees, database managers need to implement security strategies to combat the growing and varying threats posed by criminals in the rapidly changing interconnected information industry. It is crucial for database managers to develop security schemes that could address database vulnerabilities to avert system failures.

Therefore, there is a need to focus on verifying user identity. Identification measures revolve around what a user knows, like a personal identification number (PIN),

a password, or something a user has like a smart card, including something a person is like a fingerprint. It is crucial to enforce security policies. Efficient policies identify the rules and procedures for all individuals accessing and using organization database assets and resources (Cram et al., 2017). The fundamental objective of security policy is to preserve confidentiality, integrity, and availability of assets and information used by an organization. Efficient and robust encryption is required to deny data access to unlawful entities (Thomchick & San Nicolas-Rocca, 2018). Strong encryption will need a large number as its cryptographic key. Such is crucial because the more significant the key, the longer it takes to break the code unlawfully. Employees, contractors, and business associates who have information concerning the organizations' private security practices, data, and computer systems pose a serious threat. A good practice will be to use systems audits to monitor the activities of malicious and negligent insiders. Strong safeguards for external threats are needed. There is a need to address unpatched software, weak passwords, and unattended log files. Care must be taken to prevent system vulnerability. Implementing IDS, System audits, secure encryption, including anti-software programs, will help to avert external threats.

Database managers need to identify system threats and vulnerabilities, which might lead to system exposure, including measuring potential risks. Failure to address potential security dangers could lead to fraudulent claims and catastrophic system exposure (German, 2016). Fraudulent activities can expose a patient's health records, lead to treatment errors, which might result in the wrong diagnosis, including violation of Health Insurance Portability and Accountability Act regulations.

One of the outcomes from the study is an understanding that the burden of implementing data breach strategies depend on database managers who have the responsibility of employing different security layers to combat data breaches. Implementing data breach strategies could help organizations to detect, aggregate, analyze, identify, respond, contain, and recover, including finding measures of improving so that future breach occurrences will minimize. Research results from the study may provide database managers with a comprehensive understanding of data breaches, including strategies used to mitigate the effects of security incidents.

The application of study results may create a cognizance that a data breach is real and that any organization could become a victim of a security breach. Such knowledge might raise a new awareness of the dangers posed by data breach and duty of security managers in changing their attitudes when it comes to monitoring organizational databases. The results of the study could create an awareness regarding the importance of enforcing organizational security policies. Corporate security policies demand unfettered compliance from employees, vendors, contractors, including other interested parties who provide services for healthcare organizations.

Implementation of the study results might change the culture of BYOD. Often, healthcare industries may allow employees to use their devices to access organizational resources. When employees are permitted to use their tools to accomplish their job, such practice could create a security hazard. While some employees argue that BYOD saves money and resources for an organization, including helping them to be more productive, BYOD might pose security risks for an organization. Private devices could introduce

malware, virus, as well as other security vulnerabilities if such devices do not possess organizational security measures. Database managers or organizational security leaders could either restrict BYOD or enact security policies that will enforce BYOD users to comply with corporate security policies. Such compliance could counter database threats that might lead to data breaches.

Results from the study demonstrated that data breaches in healthcare industries at times might involve healthcare employees, contractors, including other healthcare partners. Therefore, strengthening security strategies, protective measures, and preventative procedures, including enforcement of organizational security policies, might help to minimize security incidents, which might lead to data breaches (White, Ekin, & Visinescu, 2017). Database managers need to provide programs, education, and training where employees, contractors, vendors, and other healthcare partners could collaborate to avoid becoming a conduit through which cybercriminals or social engineers may use to breach systems. Vast amounts of data are a significant challenge for organizations. Transmitting such data across different departments without appropriate protection like encryption might expose a patient's data, making it vulnerable to cyber scammers. Database managers need to evaluate security strategies in place to assess what's working and what's not. Such approaches could help in minimizing occasions that might lead to data breaches.

Implications for Social Change

A significant implication of this study was to minimize the volume of security breaches amongst healthcare organizations. Developing effective technical strategies

used in protecting database infrastructure could assist healthcare organizations in achieving their business objectives. Many database users do not understand how the systems work. Showing users and individuals whose data are housed in the organizational database that their information is safe will reflect a positive change. A positive change in the patient's mindset regarding data safety will build trust between patients and healthcare organizations. Having an idea that database managers are implementing appropriate security measures will prevent intruders from obtaining private information (Agelidis, 2016).

The results from the study may contribute to a positive social change in the sense the consequences might be used to educate, create awareness, or provide strategic defense measures, including training for organizational security leaders. Security strategies enable employees, contractors, and business associates to implement security solutions in a safe environment while conforming to the Health Insurance Portability and Accountability Act (HIPPA) standards (Langer, 2017). Healthcare providers will understand how to encrypt patients' information to protect the confidentiality of patient's information. Enhanced security strategies will lead to improved diagnosis and prevent medical errors because, with appropriate security strategies, cybercriminals will not be able to inject malware into diagnostic equipment, which could lead to medical failure.

The study will bring a significant change over time regarding peoples' behavior and attitudes concerning the use of information systems. For example, improved security strategies will lead to improved protection of critical information infrastructure. Significant change will lead to a better security understanding between different entities

like communication technologies, individuals, or organizations in creating enhanced security strategies to prevent cyber-attacks. Therefore, improved data security strategies could lead to secure data protection for different organizations like the department of defense, commerce, or other industries like banking, including retail stores. The technology benefit will lead to the creation of social movements. Such movements may focus on a common goal relating to activities designed to find security measures that could lead to better protection of data privacy to ensure people will not become victims of cyber-attacks. Such movements could span through different groups, individuals, organizations, or nations. The development of social movement within an organization could create chances for the development of strong leadership committed to a secure security environment, including encouraging employees and business associates to commit to recommended security policies (Kim & Scott, 2019). Technology development seen in various industries will facilitate societal improvement.

Enhanced security strategies are crucial because of its social impact. Communities that embrace dependable security strategies will engage in communal conversation regarding security intelligence. Communities involved in security intelligence can develop a security culture that could protect them from security breaches. For example, communities that focus on security strategies to maintain their sensitive data will have a more relaxed mind. When data is adequately secured, the chances of such data being compromised by cybercriminals is remote (Simmonds, 2018). Data security is an integral aspect of every culture, especially institutions involved in the business. Technology influences everyday life and has a strong influence on culture. Security strategies

improve peoples' culture regarding how they handle private data. A culture of secure data influences many facets of the global communities today, be it email, social media, or private data.

In terms of individual users, security strategies make people make informed decisions regarding how to secure private data. In our technological age, many people have critical data that is vital to their wellbeing. While personal data could be accessed anywhere in the world, users have to make a prudent decision on how to secure data from criminals (Simmonds, 2018). The increased accessibility of shared information increases the risk of external attacks. Individual users' benefits are significant. Individuals are more open to secure sensitive data with informal and formal technical approaches. The societal impact enhances users to develop a security culture and create an awareness and help them to protect their data better, including avoiding unlawful security behaviors that might lead to breaches. The implications of social change could extend to creating awareness of ethical behaviors in using IT, especially concerning data privacy. Consequently, it may help organizational leaders and policymakers understand the threats data breach might bring to industries, including providing relevant programs that could enhance data security in database systems.

The findings might equip organizational security leaders with the skills to understand different aspects of data privacy breaches to develop proactive measures that might lead to better security. The study might provide better communication and information sharing amongst database managers, including addressing occasions that could lead to data breaches.

Recommendations for Action

The purpose of the qualitative multiple case study was to explore the technical strategies used by database managers to protect systems from security breaches. Based on the information obtained from database managers during the study, a couple of issues were addressed while exploring concerns related to safeguarding databases from system weaknesses. Therefore, I recommend that database managers focus on rigorous database testing to ensure the robustness of system defenses. A failure to implement necessary patches due to excessive workload could lead to system misconfiguration, giving unmitigated access to hackers to subvert systems assurance.

I recommend that database managers engage in routine audits to document when data is amended, changed, updated, or accessed. Cybercriminals could take advantage of inadequate auditing to exploit system vulnerabilities. Significant audit tracking can deter hackers from having access to organizational databases (Mercuri & Neumann, 2016). Database managers need to pay attention to a weak password/username, extensive user privilege, broken configuration, including unpatched databases and buffer overflows (Guo & Zhang (2018). Database managers must address system weaknesses that could result in standardized query language injection. Such injections could be used to attack data-driven applications. A successful malicious standardized query language injection could destroy system defenses giving cybercriminals unfettered access to steal and alter database systems.

The findings from the study indicated that some data breaches originate from illegal activities of insiders. Therefore, I recommend that database managers engage in

regular system audit to monitor the activities of employees, provide education, and enforce corporate policies, including taking appropriate sanctions against employees who violate organizational policies. Insider threats could alter useful data, create unnecessary data duplication, including undermining security measures, thereby creating loopholes for cybercriminals to navigate systems infrastructure (Pasquale et al., 2016). Such threats could introduce malware, viruses, or worms.

To minimize external security incidents, I recommend that database managers reevaluate organizational existing security systems, including system vulnerabilities and weaknesses, to identify weak ends that could lead to security breaches. External threats such as the use of malware by cyber attackers against organizational system infrastructure represent one of the most significant external threats against organizations (Makridis & Dean, 2018). It is crucial to remove dormant users, monitor all database access activity and usage patterns to detect data leakage, including blocking malicious requests.

Finally, concerning authentication methods that are used to access databases, I recommend that two-factor authentication be reevaluated. Dedicated hackers have little problem bypassing through weaker identification measures either by intercepting codes, exploiting the account recovery system, or through keylogging techniques. Current authentication measures involving username and password may not defend against keylogging attacks (Khedr, 2018). Multiple-authentication measures, which include multiple identification measures such as username, password, including smartcard or biometrics, could offer adequate security measures (Khedr, 2018). The information could be useful to healthcare organizations that want to provide proper system security.

Recommendations for Further Study

The findings from the study provide a basis for further research in areas of securing database infrastructure from security breaches. The multiple-case study centered on two healthcare organizations in Southeast/North Texas. Participants involved in the study shared valuable information regarding strategies used to protect databases from security breaches. A data breach is a perennial problem and will continue to plague not only healthcare organizations but several other industries. There is a need to expand on this research not only from participants' viewpoint but equally by projecting the mindset of cybercriminals.

Future researchers need to explore the challenge posed by big data. Healthcare organizations generate an enormous amount of data, making it difficult for database managers to manipulate. When data sets become so large, traditional data processing applications could become problematic to handle. The difficulty in identifying the right data and determining how to best use it is a severe issue. In large databases, identifying, capturing, sharing, and transferring datasets could lead to data exposure.

It might be helpful for future researchers to investigate data breaches within nations outside of the United States. Such research might provide relevant information on how to combat data breaches originating internationally. The study focused on two healthcare systems in Southeast/North Texas and did not investigate other healthcare systems that could have suffered data breaches. Therefore, future research might try to expand their investigation to other industries such as the banking industry, department of defense, including other business industries to determine if the findings from the study

are consistent with other sectors. Granted that data saturation was reached after a ninth semi-structured face-to-face interview, including a review of organizational documents, I suggest future researchers might expand the number of participants. Such expansion may lead to new information regarding the strategies used in minimizing data breaches.

Finally, to minimize future threats posed either by insiders or cybercriminals, database managers need to understand the fundamental nature of security breaches and how employees might contribute to information exposure leading to system weaknesses. Future studies may relate to why database systems are vulnerable to security breaches, including why healthcare systems are prone to data breaches.

Reflections

The research process was very rigorous and demanding. As I embarked on the program, my goal was to gain a better understanding of how to better protect database systems from security breaches. Some friends warned me that the doctoral process is a very frustrating adventure. I chose the research area because database security is an essential investigation due to continuous and never-ending data breaches that hit the headlines. Almost every organization uses databases to store data. I felt it would be an excellent adventure to get more extensive knowledge regarding why databases are vulnerable.

I made every effort to gather all research materials and took every precaution to minimize research bias. I followed a step-by-step interview process. I was open to new ideas as I gathered information from participants. I discovered that insiders and inadequate security measures contribute to various security events that could lead to data

breaches. I gained valuable knowledge from participants regarding different security strategies used to protect database systems.

At the beginning of the research process, I thought I had reasonable insight regarding security incidents that might lead to data breaches. Nevertheless, during the research process, I appreciated new ideas and viewpoints from participants that were different from my perspectives. The process helped me to acknowledge my personal biases. Recognizing my own biases helped me in being open, transparent, including seeing the study from different standpoints.

Summary and Study Conclusions

In investigating technical strategies database managers use to protect healthcare database systems from data breaches, my objective was to uncover the dangers and risks associated with the disclosure of privacy breaches related to sensitive protected information. A data breach incident in which sensitive, protected, or confidential data is viewed or stolen by unauthorized cybercriminals may result in the compromise of personally identifiable information such as credit cards, date of births, or other identifying information. Security breaches involving a healthcare industry may result in the damage of patient health records, inaccurate medical diagnoses, wrong medication, fraudulent claims, or paralysis of healthcare database systems. Costs related to security breaches to an organization may result in millions of dollars in losses, loss of confidence, including punitive sanctions.

Considering the dangers involved in the destruction of personal privacy or sensitive protected health information, protecting healthcare database infrastructure

becomes an utmost priority for healthcare organizations. Database managers need to secure database systems against unauthorized entities. Robust authentication will be able to foil password penetration or minimize the risk of illegal intrusion. Intrusion detection systems (IDS) will be able to monitor database systems for malicious activities, including security policy violations. Encryption mechanisms will encode messages so that only authorized parties can access it. Information auditing will analyze and interpret different types of information systems within an organization. The system may develop, evaluate, and examine organizational information systems, internal controls, and management procedures to make sure records are accurate, including examining system leakage, alteration, or duplication.

Healthcare organizations can benefit when they integrate and deploy comprehensive technical security strategies. Combining different security mechanisms could save organizations enormous operational costs, including averting security incidents that might lead to data breaches. Thus, to effectively manage database systems, including combating security incidents that could lead to data breaches, database managers need to assess, measure, evaluate, and continuously monitor organizational database systems. Through the integration of comprehensive security strategies, including applicable preventative measures, database managers could minimize occasions or security events that could lead to security breaches.

References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behavior & Information Technology, 33*(3), 236-247, doi:10.1080/0144929X.2012.708787

Abdul, M., Muhammad, A. M., Mustapha, N., Muhammad, S., & Ahmad, N. (2014). Database workload management through CBR and fuzzy based characterization. *Applied Soft Computing, 22*, 605-621. doi:10.1016/j.asoc.2014.04.030

Abdullahi, A., & Orukpe, P. E. (2016). Development of an integrated campus security alerting system. *Nigerian Journal of Technology, 35*(4), 895-903. doi:10.4314/njt.v35i4.26

Abdalla, M. M., Oliveira, L. G. L., Azevedo, C. E. F., & Gonzalez, R. K. (2018). Quality in qualitative organizational research: Types of triangulation as a methodological alternative. *Administração: Ensino e Pesquisa, 19*(1), 66-98. Doi:10.13058/raep.2018.v19n1.578

Abulaish, M., & Bhat, S. Y. (2015). Classifier ensembles using structural features for spammer detection in online social networks. *Foundations of Computing & Decision Sciences, 40*(2), 89-105. Doi:10.1515/fcds-2015-0006

Adewunmi, Y. A., Koleoso, H., & Omirin, M. (2016). A qualitative investigation of benchmarking barriers in Nigeria. Benchmarking: *An International Journal, 23*(7), 1677-1696. Doi:10.1108/BIJ-06-2014-0055

Agelidis, Y. (2016). Protecting the good, the bad, and the urgly: “Exposure” data breaches and suggesting for coping with them. *Berkeley Technology Law Journal*,

311057-1078. Doi:10.15779/Z38F28K

Ahmad, A., Saad, M., & Mohaisen, A. (2019). Secure and transparent audit logs with BlockAudit. *Journal of Network and Computer Applications*, *145*. doi:10.1016/j.jnca.2019.102406

Akinwumi, D. A., Iwasokun, G. B., Alese, B. K., & Oluwadare, S. A. (2017). A review of game theory approach to cyber security risk management. *Nigerian Journal of Technology, 36*(4), 1271-1285. doi:10.4314/njt.v36i4.38

Alhouti, S., Johnson, C. M., & D'Souza, G. (2016). The complex web of values: The impact on online privacy concerns and purchase behavior. *Journal of Electronic Commerce Research*, *17*(1), 22-35. Retrieved from https://search-ebscohost-com.ezp.waldenulibrary.org

Álvarez, R., Andrade, A., & Zamora, A. (2018). Optimizing a password hashing function with hardware-accelerated symmetric encryption. *Symmetry, 10*(12), 705. doi:10.3390/sym10120705

Al-Yaseen, W. L., Othman, Z. A., & Ahmad Nazri, M. Z. (2016). Real-time intrusion detection system using multi-agent system. *IAENG International Journal of Computer Science, 43*(1), 80-90. Retrieved from https://ukm.pure.elsevier.com/en/publications/real-time-intrusion-detection-system-using-multi-agent-system

Anney, V. N. (2014). Ensuring the quality of the findings of qualitative research: Looking at trustworthiness criteria. *Journal of Empowering Trends in Educational Research and Policy Students, 5*, 272-281. Retrieved from

jeteraps.scholarlinkresearch.org

Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior*, *60*, 185-197. doi:10.1016/j.chb.2016.02.065

Asghar, H., Anwar, Z., & Latif, K. (2016). A deliberately insecure RDF-based semantic web application framework for teaching SPARQL/SPARUL injection attacks and defense mechanisms. *Computers & Security, 58*, 63-82. doi:10.1016/j.cose.2015.11.004

Ashenmacher, G. (2016). Indignity: Redefining the harm caused by data breaches. *Wake Forest Law Review*, *51*(1), 1-56. Retrieved from https://search-ebscohost-com.ezp.waldenulibrary.org

Atkins, D., Woods, M., Macklin, R., Paulus, T., & Atkins, D. P. (2016). Advancing qualitative research using qualitative data analysis software (QDAS)? Reviewing potential versus practice in published studies using ATLAS.ti and NVivo, 1994-2013. *Social Science Computer Review, 34*(5), 597-617. Retrieved from https://www.researchgate.net

Bacon, C. W., Lam, K. C., Eppelheimer, B. L., Kasamatsu, T. M., & Nottingham, S. L. (2017). Athletic trainers' perceptions of and barriers to patient care documentation: A report from the athletic training practice-based research network. *Journal of Athletic Training*, *52*(7), 667-675. doi:10.4085/1062-6050-52.3.15

Bajtoš, T., Gajdoš, A., Kleinová, L., Lučivjanská, K., & Sokol, P. (2018). Network

intrusion detection with threat agent profiling. *Security & Communication Networks*, 1-17. doi:10.1155/2018/3614093

Bargh, S., Choenni, M., & Meijer, R. (2016). On design and deployment of two privacy-preserving procedures for judicial-data dissemination. *Government Information Quarterly*, *33*(3), 481-493. doi:10.1016/j.giq.2016.06.002

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

Baskerville, R. L., & Myers, M. D. (2015). Design ethnography in information systems. *Information Systems Journal, 25*(1), 23-46. doi:10.1111/isj.12055

Bat-Erdene, M., Park, H., Li, H., Lee, H., & Choi, M. (2017). Entropy analysis to classify unknown packing algorithms for malware detection. *International Journal of Information Security*, *16*(3), 227-248. doi:10.1007/s10207-016-0330-4

Bauer, S., Bernroider, E. W., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security*, 145. doi:10.1016/j.cose.2017.04.009

Bay, M. (2017). The ethics of unbreakable encryption: Rawlsian privacy and the San Bernardino iPhone. *First Monday*, *22*(2), 1. doi:10.5210/fm.v22i2.7006

Baykara, M., Das, R., & Tuna, G. (2017). A novel symmetric encryption algorithm and its implementation. *Turkish Journal of Science & Technology*, *12*(1), 5-9. Retrieved from http://fbe.firat.edu.tr/sites/fbe.firat.edu.tr/files/5-9.pdf

Behal, S., Kumar, K., & Sachdeva, M. (2018). A generalized detection system to detect

distributed denial of service attacks and flash events for information theory metrics. *Turkish Journal of Electrical Engineering & Computer Sciences, 26*(4), 1759-1770. doi:10.3906/elk-1706-3400663-0

Benoot, C., Hannes, K., & Bilsen, J. (2016). The use of purposive sampling in a qualitative evidence synthesis: A worked example on sexual adjustment to a cancer trajectory. *BMC Medical Research Methodology, 16*, 2-12. doi:10.1186/s12874-016-0114-6

Bergmann, M. C., Dreißigacker, A., von Skarczinski, B., & Wollinger, G. R. (2018). Cyber-dependent crime victimization: The same risk for everyone? *CyberPsychology, Behavior & Social Networking, 21*(2), 84-90. doi:10.1089/cyber.2016.0727

Bhattacherjee, A., & Shrivastava, U. (2018). The effects of ICT use and ICT laws on corruption: A general deterrence theory perspective. *Government Information Quarterly*, *35*(4), 703-712. doi:10.1016/j.giq.2018.07.006

Billen, A., Madrigal, J. A., Scior, K., Shaw, B. E., & Strydom, A. (2017). Donation of peripheral blood stem cells to unrelated strangers: A thematic analysis. *Plos ONE, 12*(10), 1-16. doi:10.1371/journal.pone.0186438

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation? *Qualitative Health Research*, *26*(13), 1802–1811. doi:10.1177/1049732316654870

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

Boeren, E. (2018). The methodological underdog: A review of quantitative research in the key adult education journals. *Adult Education Quarterly, 68*(1), 63-79. doi:10.1177/0741713617739347

Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2015). Password and the evolution of imperfect authentication. *Communications of the ACM*, *58*(7), 78-87. doi:10.1145/2699390

Boyacı, Ş. D. B., & Güner, M. (2018). The impact of authentic material use on development of the reading comprehension, writing skills and motivation in language course. *International Journal of Instruction*, *11*(2), 351–368. doi:10.12973/iji.2018.11224a

Brunisholz, P., Erdene-Ochir, O., Abdallah, M., Qaraqe, K., Minier, M., & Valois, F. (2015). Network coding versus replication based resilient techniques to mitigate insider attacks for smart metering. *International Journal of Distributed Sensor Networks*, *2015*1-11. doi:10.1155/2015/737269

Burns, A., Posey, C., Roberts, T. L., & Lowry, P. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, 68190-209. doi:10.1016/j.chb.2016.11.018

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *Qualitative Report*, *21*(5), 811.

Cathro, V., O'Kane, P., & Gilbertson, D. (2017). Assessing reflection: Understanding skill development through reflective learning journals. *Education & Training,*

59(4), 427–442.

Cavusoglu, H., Cavusoglu, H., Son, J., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management*, 52385-400. doi:10.1016/j.im.2014.12.004

Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S., & Raghav Rao, H. (2016). Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. *Decision Support Systems*, 8347-56. doi:10.1016/j.dss.2015.12.007

Chandrakar, P., & Om, H. (2018). An efficient two-factor remote user authentication and session key agreement scheme using rabin cryptosystem. *Arabian Journal for Science & Engineering (Springer Science & Business Media B.V.)*, *43*(2), 661–673. doi:10.1007/s13369-017-2709-6

Chen, P. S., Yen, D. C., & Shu-Chiung, L. (2015). The classification of information assets and risk assessment: An exploratory study using the case of c-bank. *Journal of Global Information Management, 23*(4), 26-54. doi:10.4018/JGIM.2015100102

Chen, S., Tuan, M., Lee, H., & Lin, T. (2017). VLSI implementation of a cost-efficient micro control unit with an asymmetric encryption for wireless body sensor networks. *Ieee Access*, 54077-4086.

Chen, X., Wu, D., Chen, L., & Teng, J. K. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and

control variables. *Information & Management*, doi:10.1016/j.im.2018.05.011

Choi, B. C., Kim, S. S., & Jiang, Z. (2016). Influence of firm's recovery endeavors upon privacy breach on online customer behavior. *Journal of Management Information Systems*, *33*(3), 904-933. doi:10.1080/07421222.2015.1138375

Choi, H., Jeong, J., Woo, S. S., Kang, K., & Hur, J. (2018). Password typographical error resilience in honey encryption. *Computers & Security*. doi:10.1016/j.cose.2018.07.020

Chua, H. N., Wong, S. F., Low, Y. C., & Chang, Y. (2018). Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. *Telematics and Informatics*, *35*(6), 1770–1780. doi:10.1016/j.tele.2018.05.005

Civitillo, S., Juang, L. P., Badra, M., & Schachner, M. K. (2019). The interplay between culturally responsive teaching, cultural diversity beliefs, and self-reflection: A multiple case study. *Teaching and Teacher Education, 77*, 341–351. doi:10.1016/j.tate.2018.11.002

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

Cohen, A., Nissim, N., & Elovici, Y. (2018). Novel set of general descriptive features for enhanced detection of malicious emails using machine learning methods. *Expert Systems with Applications, 110,* 143–169. doi:10.1016/j.eswa.2018.05.031

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

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, *6*(23), 31-38. doi:10.19101/IJACR.2016.623006

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. 10.1057/s41303-017-0059-9

Cronin, C. (2014). Using case study research as a rigorous form of inquiry. *Nurse Researcher, 21*(5), 19-27. doi:10.7748/nr.21.5.19.e1240

Dadsena, K. K., Naikan, V. A., & Sarmah, S. P. (2016). A Methodology for risk assessment and formulation of mitigation strategies for trucking industry. *International Journal of Performability Engineering*, *12*(6), 573-588.

Dai, S., Li, H., & Zhang, F. (2016). Memory leakage-resilient searchable symmetric encryption. *Future Generation Computer Systems*, 6276-84. doi:10.1016/j.future.2015.11.003

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017). Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace. *Computers in Human Behavior*, *67*196-206. doi:10.1016/j.chb.2016.10.025

Dasgupta, D., Roy, A., & Nag, A. (2016). Toward the design of adaptive selection strategies for multi-factor authentication. *Computers & Security*, 6385-116. doi:10.1016/j.cose.2016.09.004

de Gusmão, A. P. H., e Silva, L. C., Silva, M. M., Poleto, T., & Costa, A. P. C. S. (2016).

Information security risk analysis model using fuzzy decision theory. *International Journal of Information Management*, *36*(1), 25–34. doi:10.1016/j.ijinfomgt.2015.09.003

Densham, B. (2015). Three cyber-security strategies to mitigate the impact of a data breach. *Network Security*, *2015*(1), 5-8. doi:10.1016/S1353-4858(15)70007-3

Derhab, A., & Bouras, A. (2016). Lightweight anomaly-based intrusion detection system for multi-feature traffic in wireless sensor networks. *Adhoc & Sensor Wireless Networks, 30*(3/4), 201-217

Di, X., Li, J., Qi, H., Cong, L., & Yang, H. (2017). A semi-symmetric image encryption scheme based on the function projective synchronization of two hyperchaotic systems. *Plos ONE*, (9), doi:10.1371/journal.pone.0184586

Dikko, M. (2016). Establishing construct validity and reliability: Pilot testing of a qualitative interview for research in Takaful (Islamic Insurance). *Qualitative Report*, *21*(3), 521-528.

Drljača, D., & Latinović, B. (2016). Frameworks for audit of an information system in practice. *Journal of Information Technology & Applications*, *6*(2), 78-85. doi:10.7251/JIT1602078D

Durkota, K., Lisy, V., Kiekintveld, C., Bosansky, B., & Pechoucek, M. (2016). Case studies of network defense with attack graph games. *IEEE Intelligent Systems*, *31*(5), 24-30. doi:10.1109/MIS.2016.74

El Said, G. R. (2017). Understanding how learners use massive open online courses and why they drop out: Thematic analysis of an interview study in a developing

country. *Journal of Educational Computing Research*, *55*(5), 724-752. doi:10.1177/0735633116681302

Elo, S., Kaariainen, M., Kanste, O., Polkki, T., Utrianen, K., & Kyngas, H. (2014). Qualitative content analysis: A focus on trustworthiness. *SAGE Open, 4*(1). doi:10.1177/2158244014522633

Eranova, M., & Prashntham, S. (2016). Decision making and paradox: Why study China? *European Management Journal, 34*(3), 193-201.

Esiner, E., & Datta, A. (2019). Two-factor authentication for trusted third party free dispersed storage. *Future Generation Computer Systems*, *90*, 291–306. doi:10.1016/j.future.2018.08.001

Fan, Y., Ye, Y., & Chen, L. (2016). Malicious sequential pattern mining for automatic malware detection. *Expert Systems with Applications*, 5216-25. doi:10.1016/j.eswa.2016.01.002

Faronbi, J. O., Faronbi, G. O., Ayamolowo, S. J., & Olaogun, A. A. (2019). Caring for the seniors with chronic illness: The lived experience of caregivers of older adults. *Archives of Gerontology and Geriatrics, 82*, 8–14. doi:10.1016/j.archger.2019.01.013

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

Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security*, *61*169-183.

doi:10.1016/j.cose.2016.06.002

Fonseca, J., Seixas, N., Vieira, M., & Madeira, H. (2014). Analysis of field data on web security vulnerabilities. *IEEE Transaction on Dependable & Secure Computing*, *11*(2), 89-100. doi:10.1109/TDSC.2013.37

Fonseca, J., Vieira, M., & Madeira, H. (2014). Evaluating of web security mechanisms using vulnerability & attack injection. *IEEE Transactions on Dependable & Secure Computing*, *11*(5), 440-453. doi:10.1109/TDSC.2013.45

Furnell, S., Khern-am-nuai, W., Esmael, R., Yang, W., & Li, N. (2018). Enhancing security behaviour by supporting the user. *Computers & Security, 75*, 1–9. doi:10.1016/j.cose.2018.01.016

Fusch, P. L., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *Qualitative Report*, 20(19), 1408-1416. Retrieved from http://tqr.nova.edu/

Galdi, C., Nappi, M., Dugelay, J.-L., & Yong, Y. (2018). Exploring new authentication protocols for sensitive data protection on smartphones. (2018). *IEEE Communications Magazine, Communications Magazine, IEEE, IEEE Commun. Mag*, (1), 136. doi:10.1109/MCOM.2017.1700342

Gandotra, E., Bansal, D., & Sofat, S. (2017). A Framework for generating malware threat intelligence. *Scalable Computing: Practice & Experience*, *18*(3), 195–205. doi10.12694/scpe.v18i3.1300

Gao, X., Zhong, W., & Mei, S. (2015). Security investment and information sharing under an alternative security breach probability function. *Information Systems*

Frontiers, 17(2), 423-438. doi:10.1007/s10796-013-9411-3

Genge, B., Kiss, I., & Haller, P. (2015). A system dynamics approach for assessing the impact of cyber-attacks on critical infrastructures. *International Journal on Critical Infrastructure Protection*, *10*3-17. doi:10.1016/j.ijcip.2015.04.001

Gergen, K. J., Josselson, R., & Freeman, M. (2015). The promises of qualitative inquiry. *American Psychologist, 70*, 1. doi:10.1037/a0038597

German, P. (2016). A new month, a new data breach. *Network Security*, *2016*(3), 18-20. doi:10.1016/S1353-4858(16)30029-0

Ghosh, P. (2014). A Framework of email cleansing and mining with case study on image spamming. *International Journal of Advanced Computer Research, 4*(17), 961-965.

Greengard, S. (2016). Cybersecurity gets smart. *Communications of the ACM, 59*(5), 29-31. doi:10.1145/2898969

Guo, H., Cheng, H. K., & Kelley, K. (2016). Impact of network structure on malware propagation: A Growth curve perspective. *Journal of Management Information Systems, 33*(1), 296-325. doi:10.1080/07421222.2016.1172440

Guo, Y., & Zhang, Z. (2018). LPSE: Lightweight password-strength estimation for password meters. *Computers & Security, 73*, 507–518. doi:10.1016/j.cose.2017.07.012

Gwebu, K. L., Jing, W., & LI, W. (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems*, *35*(2), 683-714. doi:10.1080/07421222.2018.1451962

Haahr, A., Norlyk, A., & Hall, E. O. (2014). Ethical challenges embedded in qualitative research interviews with close relatives. *Nursing Ethics, 21*, 6-15. doi:10.1177/0969733013486370

Hagaman, A. K., & Wutich, A. (2017). How many interviews are enough to identify metathemes in multisited and cross-cultural research? Another perspective on Guest, Bunce, & Johnson's (2006) landmark study. *Field Methods, 29*(1), 23-41.

Haislip, J. Z., Peters, G. F., & Richardson, V. J. (2016). The effect of auditor IT expertise on internal controls. *International Journal of Accounting Information Systems*, *20*1-15. doi:10.1016/j.accinf.2016.01.001

Hajamydeen, A. I., Udizir, N. I., Mahmod, R., & Abdul Ghani, A. A. (2016). An unsupervised heterogeneous log-based framework for anomaly detection. *Turkish Journal of Electrical Engineering & Computer Sciences, 24*(3), 1117-1134. doi:10.3906/elk-1302-19

Han, J., Kim, Y. J., & Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security*, *66*52-65. doi:10.1016/j.cose.2016.12.016

Hancock, M. E., Amankwaa, L., Revell, M. A., & Mueller, D. (2016). Focus group data saturation: A new approach to data analysis. *Qualitative Report*, *21*(11), 2124.

Handwerker, S. M. (2018). Challenges experienced by nursing students overcoming one course failure: A phenomenological research study. *Teaching and Learning in Nursing*, *13,* 168-173. doi:10.1016/j.teln.2018.03.007

Haoxing, L., Fenghua, L., Chenggen, S., & Yalong, Y. (2015). Towards smart card based

mutual authentication schemes in cloud computing. *KSII Transactions on Internet & Information Systems, 9*(7), 2719-2735. doi:10.383/tiis.2015.07.022

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, *73*, 102–113. doi:10.1016/j.cose.2017.10.008

Haydon, G., Browne, G., & van der Riet, P. (2018). Narrative inquiry as a research methodology exploring person centred care in nursing. *Collegian, 25*(1), 125-129.

Heartfield, R., & Loukas, G. (2015). A Taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Computing Surveys*, *48*(3), 37:1-37:39. doi:10.1145/2835375

Hemphill, T. A., & Longstreet, P. (2016). Financial data breaches in the U.S. retail economy: Restoring confidence in information technology security standards. *Technology in Society*, 4430-38. doi:10.1016/j.techsoc.2015.11.007

Hemkens, L. G., Contopoulos-Ioannidis, D. G., & Ioannidis, J. P. (2016). Routinely collected data and comparative effectiveness evidence: Promises and limitations. *Canadian Medical Association Journal, 188*(8), E158-E164. doi:10.1503/cmaj.150653

Hills, K. N. (2015). *Communication strategies to generate employee job satisfaction* (Doctoral Dissertation). Retrieved from ProQuest Dissertations & Thesis Full Text Database. (Order No, 3731850).

Ho, S. M., Kaarst, B. M., & Benbasat, I. (2018). Trustworthiness attribution: Inquiry into insider threat detection. *Journal of the Association for Information Science & Technology*, *69*(2), 271–280. doi:10.1002/asi.23938

Holm, H., & Afridi, K. K. (2015). An expert-based investigation of the common vulnerability scoring system. *Computers & Security*, 5318-30. doi:10.1016/j.cose.2015.04.012

Hong, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (2003). An integrated system theory of information security management. *Information Management & Computer Security, 11*(5), 243-248. doi: 10.1108/09685220310500153

Hong, K.-S., Chi, Y.-P., Chao, L. R., & Tang, J.-H. (2006). An empirical study of information security policy on information security elevation in Taiwan. *Information Management & Computer Security*, *14*(2), 104– 115. doi. 10.1108/09685220610655861

Hovav, A., & Putri, F. F. (2016). This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive and Mobile Computing, 32,* 35-49. doi:10.1016/j.pmcj.2016.06.007

Hussain, K., Jhanjhi, N., Mati-ur-Rahman, H., Hussain, J., & Islam, M. H. (2019). Using a systematic framework to critically analyze proposed smart card based two factor authentication schemes. *Journal of King Saud University - Computer and Information Sciences*. doi:10.1016/j.jksuci.2019.01.015

Hussein, A. (2015). The use of triangulation in social sciences research: Can qualitative and quantitative methods be combined? *Journal of Comparative Social Work*, 4, 1

Hwang, I., & Cha, O. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior, 81,* 282–293. doi:10.1016/j.chb.2017.12.022

Ifinedo, P., & Usoro, A. (2016). Student intentions to continue using blogs to learn. A socio-cognitive perspective. *Computing & Information Systems, 20*(3), 14-24

Iivari, N. (2018). Using member checking in interpretive research practice: A hermeneutic analysis of informants' interpretation of their organizational realities. *Information Technology & People*, (1), 111. doi:10.1108/ITP-07-2016-0168

Ikhalia, E., Serrano, A., Bell, D., & Arreymbi, J. (2017). Developing and implementing ttat-mip for the avoidance of malware threats through online social networks. *IADIS International Journal on WWW/Internet*, *15*(1), 31–46.

Ikram, S. T., & Cherukuri, A. K. (2016). Improving accuracy of intrusion detection model using PCA and optimized SVM. *Journal of Computing & Information Technology, 24*(2), 133-148. doi:10.20532/cit.2016.1002701

Ismail, S., Sitnikova, E., & Slay, J. (2014). Using integrated system theory approach to access security for SCADA systems cyber security for critical infrastructure: A pilot study. *International Conference on Fussy Systems and Knowledge Discovery (FSKD)*, 1000-1006. doi:10.1109/fskd.2014.6980976

Jain, A., & Gupta, B. (2016). A novel approach to protect against phishing attacks at client side using auto-updated white-list. *EURASIP Journal on Information Security, 2016*(1), 1-11. doi:10.1186/s13635-016-0034-3

Jiang, Q., Khan, M., Lu, X., Ma, J., & He, D. (2016). A privacy preserving three-factor authentication protocol for e-Health clouds. *Journal of Supercomputing, 72*(10), 3826-3849. doi:10.1007/s11227-015-1610-x

Jingguo, W., Gupta, M., & Rao, H. R. (2015). Insider threats in a financial institution: Analysis of attack-proneness of information systems applications. *MIS Quarterly*, *39*(1), 91-A7.

Jiping, L., Yaoming, D., Zenggang, X., & Shouyin, L. (2017). An improved two-factor mutual authentication scheme with key agreement in wireless sensor networks. *KSII Transactions on Internet & Information Systems, 11*(11), 5556-5573. doi:10.3837/tiis.2017.11.021

Joslin, R., & Müller, R. (2016). Identifying interesting project phenomena using philosophical and methodological triangulation. *International Journal of Project Management*, 34, 1043-1056. doi:10.1016/j.ijproman.2016.05.005

Kar, D., Panigrahi, S., & Sundararajan, S. (2016). SQLiGoT: Detecting SQL injection attacks using graph of tokens and SVM. *Computers & Security*, 60206-225. doi:10.1016/j.cose.2016.04.005

Karlsson, F., Hedström, K., & Goldkuhl, G. (2017). Practice-based discourse analysis of information security policies. *Computers & Security*, 67, 267-279. doi:10.1016/j.cose.2016.12.012

Ke, L. (2016). Integrating ethical guidelines and situated ethics for researching social-media-based interactions. *Journal of Information Ethics*, *25*(1), 114-131.

Kerwin-Boudreau, S., & Butler-Kisber, L. (2016). Deepening Understanding in Qualitative Inquiry. *Qualitative Report, 21*(5), 956-971.

Khedr, W. I. (2018). Improved keylogging and shoulder-surfing resistant visual two-factor authentication protocol. *Journal of Information Security and Applications*,

3941-57. doi:10.1016/j.jisa.2018.02.003

Kim, D. W., Yan, P., & Zhang, J. (2015). Detecting fake anti-virus software distribution webpages. *Computers & Security*, 4995-106. doi:10.1016/j.cose.2014.11.008

Kim, H., & Scott, C. (2019). Change communication and the use of anonymous social media at work : Implications for employee engagement. *Corporate Communications: An International Journal*, (3), 410. doi:10.1108/CCIJ-07-2018-0076

King, K. M., Pullmann, M. D., Lyon, A. R., Dorsey, S., & Lewis, C. C. (2019). Using implementation science to close the gap between the optimal and typical practice of quantitative methods in clinical science. *Journal of Abnormal Psychology*, *128*(6), 547–562. doi:10.1037/abn0000417

Kirkpatrick, K. (2015). Cyber policies on the rise. *Communications of the ACM, 58*(10), 21-23. doi:10.1145/2811290

Krajnović, D. M., & Jocić, D. D. (2017). Experience and attitudes toward informed consent in pharmacy practice research: Do pharmacists care? *Science and Engineering Ethics, 23*(6), 1529–1539. doi:10.1007/s11948-016-9853-3

Kumari, S., & Om, H. (2015). Remote login authentication scheme based on bilinear pairing and fingerpoint. *KSII Transactions on Internet & Information Systems, 9*(12), 4987-5014. doi:10.3837/tiis.2015.12.014

Langer, S. G. (2017). Cyber-security issues in healthcare information technology. *Journal of Digital Imaging*, *30*(1), 117–125. doi:10.1007/s10278-016-9913-x

Lasrado, F., & Uzbeck, C. (2017). The excellence quest: a study of business excellence award-winning organizations in UAE. *Benchmarking: An International Journal*, *24*(3), 716-734. doi:10.1108/BIJ-06-2016-0098

Lawrence, A., Minutti-Meza, M., & Vyas, D. (2018). Is operational control risk informative of financial reporting deficiencies? Auditing: *A Journal of Practice & Theory, 37*(1), 139–165. doi:10.2308/ajpt-51784

Lee, H., Lim, D., Kim, H., Zo, H., & Cigaek, A. P. (2015). Compensation paradox: the influence of monetary rewards on user behaviour. *Behaviour & Information Technology*, *34*(1), 45-56. doi:10.1080/0144929X.2013.805244

Lee, T., & Kwak, J. (2016). Effective and reliable malware group classification for a massive malware environment. *International Journal of Distributed Sensor Networks,* 1-6. doi:10.1155/2016/4601847

Leedy, P. D., & Ormrod, J. E. (2015). *Practical research: Planning and design* (11th ed.). New York, NY: Pearson.

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

Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health Promotion Practice*, *16*, 473-475. doi:10.1177/1524839915580941

Li, P., Chan, D. Y., & Kogan, A. (2016). Exception prioritization in the continuous auditing environment: a framework and experimental evaluation. *Journal of*

Information Systems, *30*(2), 135-157. doi:10.2308/isys-51220

Li, W., Meng, W., Kwok, L., & Ip, H. H. (2017). Enhancing collaborative intrusion detection networks against insider attacks using supervised intrusion sensitivity-based trust management model. *Journal of Network & Computer Applications*, 77135-145. doi:10.1016/j.jnca.2016.09.014

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly, 33*(1), 71-90

Liang, N., Biros, D. P., & Luse, A. (2016). An empirical validation of malicious insider characteristics. *Journal of Management Information Systems*, *33*(2), 361-392. doi:10.1080/07421222.2016.1205925

Lijiao, C., Wenli, L., Qingguo, Z., & Smyth, R. (2014). Understanding personal use of the internet at work: An integrated model of neutralization techniques and general deterrence theory. *Computers in Human Behavior*, 38220-228. doi:10.1016/j.chb.2014.05.043

Liu, J., Lyu, Q., Wang, Q., & Yu, X. (2017). A digital memories based user authentication scheme with privacy preservation. *Plos ONE*, *12*(11), 1-22. doi:10.1371/journal.pone.0186925

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

Lowry, P. B., Posey, C., Bennett, R. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced

organizational information security policies: An empirical study of the influence of counterfactual reasoning and organizational trust. *Information Systems Journal, 25*(3), 193-273. doi:10.1111/isj.12063

Lu, N., Sun, Y., Liu, H., & Li, S. (2018). Intrusion detection system based on evolving rules for wireless sensor networks. *Journal of Sensors*, 1-8. doi:10.1155/2018/5948146

Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2016). Cyber threats to health information systems: A systematic review. *Technology & Health Care*, *24*(1), 1-9. doi:10.3233/THC-151102 Lyle, J. (2018). The transferability of sport coaching research: A critical commentary. *QUEST*, *70*(4), 419–437. doi:10.1080/00336297.2018.1453846

Makridis, C., & Dean, B. (2018). Measuring the economic effects of data breaches on firm outcomes: Challenges and opportunities. *Journal of Economic & Social Measurement, 43*(1/2), 59–83. doi:10.3233/JEM-180450

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

Marshall, C., & Rossman, G. (2016). *Designing qualitative research (*6th ed.). Washington DC: Sage.

Martins, P., Sousa, L., & Mariano, A. (2017). A survey on fully homomorphic encryption: An engineering perspective. *ACM Computing Surveys*, *50*(6), 1-33. doi:10.1145/3124441

May, J., & Lending, D. (2015). A conceptual model for communicating an integrated information systems curriculum. *Journal of Computer Information Systems, 55*(4), 20-27.

Mazur, K., Ksiezopolski, B., & Nielek, R. (2016). Multilevel modeling of distributed denial of service attacks in wireless sensor networks. *Journal of Sensors*, 1-13. doi:10.1155/2016/5017248

McKeown, E., & Storm-Smith, E. (2016). New legislation strengthens legal protections for cybersecurity information-sharing. *Intellectual Property & Technology Law Journal, 28*(5), 17-19.

Mercuri, R. T., & Neumann, P. G. (2016). The risks of self-auditing Systems. *Communications of the ACM*, *59*(6), 22-25. doi:10.1145/2909877

Midi, D., Sultana, S., & Bertino, E. (2016). A system for response and prevention of security incidents in wireless sensor networks. *ACM Transactions on Sensor Networks*, *13*(1), 1-38. doi:10.1145/2996195

Mitchell, J. (2015). Risk Assessment. *Itnow*, *57*(1), 14-15.

Mol, A. M., Silva, R. S., Rocha, Á. A., & Ishitani, L. (2017). Ethnography and Phenomenology applied to game research: a systematic literature review. *Revista De Sistemas E Computação (RSC)*, *7*(2), 110-127.

Monahan, T., & Fisher, J. A. (2015). Strategies for obtaining access to secretive or guarded organizations. *Journal of Contemporary Ethnography, 6*, 709.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*(1), 285-A22.

Movahedi, Y., Cukier, M., Andongabo, A., & Gashi, I. (2019). Cluster-based vulnerability assessment of operating systems and web browsers. *Computing, 101*(2), 139–160. doi:10.1007/s00607-018-0663-0

Murtaza, S. S., Khreich, W., Hamou-Lhadi, A., & Bener, A. B. (2016). Mining trends and patterns of software vulnerabilities. *Journal of Systems & Software*, 117218-228. doi:10.1016/j.jss.2016.02.048

Nandi, A. K., Medal, H. R., & Vadlamani, S. (2016). Interdicting attack graphs to protect organizations from cyber-attacks: A bi-level defender–attacker model. *Computers & Operations Research*, 75118-131. doi:10.1016/j.cor.2016.05.005

Nasir, A., Arshah, R. A., Hamid, M. R. A., & Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. *Journal of Information Security and Applications*, *44*, 12–22. doi:10.1016/j.jisa.2018.11.003

Nelson, A. M. (2016). Methodology for examining attributes of African Americans in the department of defense senior executive service Corp. *Journal of Economic Development, Management, IT, Finance & Marketing*, *8*(1), 48-68.

Odelu, V., Das, A. K., & Goswami, A. (2016). A secure effective dynamic group password-based authenticated key agreement scheme for the integrated EPR information system. *Journal of King Saud University - Computer and Information Sciences*, *28*(1), 68–81. doi:10.1016/j.jksuci.2014.04.008

Otero, A. R. (2015). An information security control assessment methodology for organizations' financial information. *International Journal of Accounting Information Systems*, 1826-45. doi:10.1016/j.accinf.2015.06.001

Ozair, F. F., Jamshed, N., Sharma, A., & Aggarwal, P. (2015). Ethical issues in electronic health records: A general overview. *Perspectives in Clinical Research*, *6*, 73-76. doi:10.4103/2229-3485.153997

Padayachee, K. (2016). An assessment of opportunity-reducing techniques in information security: An insider threat perspective. *Decision Support Systems*, 9247-56. doi:10.1016/j.dss.2016.09.012

Miss, P., Sinha, A., Shrivastava, G., & Kumar, P. (2019). A pattern-based multi-factor authentication system. Scalable computing: *Practice & Experience, 20*(1), 101–112. doi:10.12694/scpe.v20i1.1460

Park, Y., Park, K., Park, Y., Lee, K., & Song, H. (2017). Security analysis and enhancements of an improved multi-factor biometric authentication scheme. *International Journal of Distributed Sensor Networks*, *13*(8)

Pasquale, L., Hanvey, S., Mcgloin, M., & Nuseibeh, B. (2016). Adaptive evidence collection in the cloud using attack scenarios. *Computers & Security*, *59*236-254. doi:10.1016/j.cose.2016.03.001

Patino, C. M., & Ferreira, J. C. (2018). Internal and external validity: can you apply research study results to your patients? *Jornal Brasileiro De Pneumologia*, *44*(3), 183. doi:10.1590/S1806-37562018000000164

Perry, L., James, S., Gallagher, R., Dunbabin, J., Steinbeck, K., & Lowe, J. (2017). Supporting patients with type 1 diabetes using continuous subcutaneous insulin infusion therapy: Difficulties, disconnections, and disarray. *Journal of Evaluation in Clinical Practice*, *23*(4), 719-724.

Peters, K., & Halcomb, E. (2015). Interviews in qualitative research: A consideration of two different issues in the use of interviews to collect research data. *Nurse Researcher, 22*, 6-7. doi:10.7748/nr.22.4.6.s2

Poh, G. S., Chin, J. J., Yau, WC., Choo, K-K.R., & Mohamad, M. S. (2017). Searchable symmetric encryption: Designs and challenges. *ACM Computing Surveys*, *50*(3), 40:1-40:37. doi:10.1145/3064005

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management*, *51*(5), 551–567. doi:10.1016/j.im.2014.03.009

Pozzebon, M., & Rodriguez, C. (2014). Dialogical principals for qualitative inquiry: A nonfoundational path. *International Journal of Qualitative Methods, 2014*(13), 293-317.

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

Rafferty, B. (2016). Dangerous skills gap leaves organizations vulnerable. *Network Security, 2016*(8), 11-13. doi:10.1016/S1353-4858(16)30077-0

Rahimian, F., Bajaj, A., & Bradley, W. (2016). Estimation of deficiency risk and prioritization of information security controls: A data-centric approach. *International Journal of Accounting Information Systems*, *20*38-64. doi:10.1016/j.accinf.2016.01.004

Rajab, M., & Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security*, *80*, 211–223. doi:10.1016/j.cose.2018.09.016

Renz, S. M., Carrington, J. M., & Badger, T. A. (2018). Two strategies for qualitative content analysis: An intramethod approach to triangulation. *Qualitative Health Research, 28*(5), 824-831. doi:10.1177/1049732317753586

Richardson, R. (2015). Disambiguating database. *Communications of the ACM, 58*(1), 54-61. doi:10.1145/2687880

Rikhardsson, P., & Dull, R. (2016). An exploratory study of the adoption, application and impacts of continuous auditing technologies in small businesses. *International Journal of Accounting Information Systems*, *20*26-37. doi:10.1016/j.accinf.2016.01.003

Rodríguez, A., Ortega, F., & Concepción, R. (2017). An intuitionistic method for the selection of a risk management approach to information technology projects. *Information Sciences*, *375*202-218. doi:10.1016/j.ins.2016.09.053

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

Rubino, M., Vitolla, F., & Garzoni, A. (2017). The impact of an IT governance framework on the internal control environment. *Records Management Journal*, *27*(1), 19-41. doi:10.1108/RMJ-03-2016-0007

Ruckman, S. M., & Dhaliwal, A. S. (2015). The FCC'S expanding definition of privacy. *Journal of Internet Law*, *19*(4), 1-10.

Run-hua, S., Hong, Z., Jie, C., & Shun, Z. (2015). A novel one-to-many and many-to-one asymmetric encryption model and its algorithms. *Security & Communication Networks, 8*(18), 3906-3913. doi:10.1002/sec.1309

Ruohonen, J. (2017). Original Article: A look at the time delays in CVSS vulnerability scoring. *Applied Computing and Informatics*, doi:10.1016/j.aci.2017.12.002

Ruohonen, J., Rauti, S., Hyrynsalmi, S., & Leppänen, V. (2018). A case study on software vulnerability coordination. *Information and Software Technology, 103*, 239–257. doi:10.1016/j.infsof.2018.06.005

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, 57442-451. doi:10.1016/j.chb.2015.12.037

Sampaio, L., & Garcia, A. (2016). Exploring context-sensitive data flow analysis for early vulnerability detection. *The Journal of Systems & Software*, 113337-361. doi:10.1016/j.jss.2015.12.021

Sampemane, G. (2015). Internal access controls. *Communications of the ACM*, *58*(1), 62-65. doi:10.1145/2687878

Saravana Kumar, N., Deepa, S., Marimuthu, C., Eswari, T., & Lavanya, S. (2016). Signature based vulnerability detection over wireless sensor network for reliable data transmission. *Wireless Personal Communications*, *87*(2), 431-442. doi:10.1007/s11277-015-3070-2

Schuessler, J. H., Nagy, D., Fulk, H. K., & Dearing, A. (2017). Data breach laws: Do they work? *Journal of Applied Security Research, 12*(4), 512-524.

doi:10.1080/19361610.2017.1354275

Scrutton, R., & Beames, S. (2015). Measuring the unmeasurable: Upholding rigor in quantitative studies of personal and social development in outdoor adventure education. *Journal of Experiential Education*, *38*, 8-25. doi:10.1177/1053825913514730

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems, 32*(2), 314-341. doi:10.1080/07421222.2015.1063315

Senate bill proposes data privacy, security obligations. (2015). *Journal of Internet Law*, *18*(12), 13.

Serra, E., Jajodia, S., Pugliese, A., Rullo, A., & Subrahmanian, V. S. (2015). Pareto-optimal adversarial defense of enterprise systems. *ACM Transactions on Information & System Security* (*TISSEC*), *17*(3), 1-39. doi:10.1145/2699907

Shaji, N. A., & Soman, S. (2017). Multi-factor authentication for net banking. *International Journal of System & Software Engineering, 5*(1), 11-14.

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security*, 5714-30. doi:10.1016/j.cose.2015.11.001

Sharma, A., Parveen, S., & Misra, P. (2016). Misuse detection system using intelligent agents for online transactions. *BVICAM's International Journal of Information Technology, 8*(1), 955-958.

Sharma, S., & Warkentin, M. (2018). Do I really belong? Impact of employment status

on information security policy compliance. *Computers & Security*. doi:10.1016/j.cose.2018.09.005

Siadati, H., Nguyen, T., Gupta, P., Jakobsson, M., & Memon, N. (2017). Mind your SMSes: Mitigating social engineering in second factor authentication. *Computers & Security*, *65,* 14-28. doi:10.1016/j.cose.2016.09.009

Sicari, S., Rizzardi, A., Miorandi, D., Cappiello, C., & Coen-Porisini, A. (2016). Security policy enforcement for networked smart objects. *Computer Networks*, 108133-147. doi:10.1016/j.comnet.2016.08.014

Simab, M., Chatrsimab, S., Yazdi, S., & Simab, A. (2017). A new method for power system contingency ranking using combination of neural network and data envelopment analysis. *Journal of Intelligent & Fuzzy Systems*, *32*(6), 3859-3866. doi:10.3233/IFS-162169

Simmonds, M. (2018). Instilling a culture of data security throughout the organisation. *Network Security*, *2018*(6), 9–12. doi:10.1016/S1353-4858(18)30055-2

Small, W., Maher, L., & Kerr, T. (2014). Institutional ethical review and ethnographic research involving injection drug users: A case study. *Social Science & Medicine*, *104*, 157–162. doi:10.1016/j.socscimed.2013.12.010

Smith, S. P., & Johnston, R. B. (2014). How critical realism clarifies validity issues in information systems theory-testing research. *Scandinavian Journal of Information Systems, 26*(1), 5-27.

Smyth, G. (2017). Using data virtualisation to detect an insider breach. *Computer Fraud*

& Security, *2017*(8), 5–7. doi:10.1016/S1361-3723(17)30068-4

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, 5670-82. doi:10.1016/j.cose.2015.10.006

Soltanizadeh, S., Abdul Rasid, S. Z., Mottaghi Golshan, N., & Wan Ismail, W. K. (2016). Business strategy, enterprise risk management and organizational performance. *Management Research Review, 39*(9), 1016-1033. doi:10.1108/MRR-05-2015-0107

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215-225. doi:10.1016/j.ijinfomgt.2015.11.009

Sonuga, B. E. (2017). Editorial: Science unskewed—acknowledging and reducing 'risk of bias' in parenting research. *Journal of Child Psychology and Psychiatry, 58*(1), 1–3. doi:10.1111/jcpp.12676

Spafford, E. H. (2016). The strength of encryption. *Communications of the ACM*, 59(3), 5. doi:10.1145/2889284

Spiers, J., Morse, J. M., Olson, K., Mayan, M., & Barrett, M. (2018). Reflection/commentary on a past article: "Verification strategies for establishing reliability and validity in qualitative research." *International Journal of Qualitative Methods, 17*(1). doi:10.1177/1609406918788237

Srivastava, H., & Kumar, S. A. (2015). Control framework for secure cloud computing. *Journal of Information Security*, *6,* 12-23. doi:10.4236/jis.2015.61002

Steinbart, P. J., Raschke, R. L., Gal, G., William, N., & Dilla, W. N. (2016). SECURQUAL: An instrument for evaluating the effectiveness of enterprise information security programs. *Journal of Information Systems, 30* (1), 71-92. doi:10.2308/isys-51257

Stiawan, D., Idris, M. Y., Abdullah, A. H., Aljaber, F., & Budiarto, R. (2017). Cyber-attack penetration test and vulnerability analysis. *International Journal of Online Engineering*, *13*(1), 125-132. doi:10.3991/ijoe.v13i01.6407

Tan, X., & Yu, F. (2018). Research and application of virtual user context information security strategy based on group intelligent computing. *Cognitive Systems Research*, *52*, 629–639. doi:10.1016/j.cogsys.2018.08.016

Thiele, T., Pope, D., Singleton, A., & Stanistreet, D. (2018). Exploring the use of mixed methods in research and evaluation of widening participation interventions: Guidance for practitioners. *Widening Participation & Lifelong Learning, 20*(4), 7–38. doi:10.5456/WPLL.20A.7

Thomchick, R., & San Nicolas-Rocca, T. (2018). Application level security in a public library: A case study. *Information Technology & Libraries, 37*(4), 107–118. doi:10.6017/ital.v37i4.10405

Toxen, B. (2014). The NSA and Snowden: Securing the all-seeing eye. *Communications of the ACM*, *57*(5), 44-51. doi:10.1145/2594502

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, 59138-150. doi:10.1016/j.cose.2016.02.009

Tsung-Han, Y., Cheng-Yuan, K., & Man-Nung, L. (2016). An integrated system for information security management with the unified framework. *Journal of Risk Research, 19* (1) 21–41. doi.org/10.1080/13669877.2014.940593

Twining, P., Heller, R. S., Nussbaum, M., & Tsai, C. (2017). Some guidance on conducting and reporting qualitative studies. *Computers & Education*, *106*, A1-A9. doi:10.1016/j.compedu.2016.12.002

Tyler, J. (2016). Feature: Don't be your own worst enemy: protecting your organization from inside threats. *Computer Fraud & Security*, *2016*19-20. doi:10.1016/S1361-3723(16)30063-X

U.S. Department of Health and Human Services. (1979). *The Belmont Report*. Retrieved from http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html#xrespect

Vance, A., Lowry, P. B., & Eggett, D. (2015). A new approach to the problem of access policy violations: Increasing perceptions of accountability through the user interface. *MIS Quarterly, 39*(2), 345-366.

Van der Vyver, A. G., & Marais, M. (2015). Evaluating users' perceptions of the digital doorway: A narrative analysis. *Information Technology for Development, 21*(1), 99-112. doi:10.1080/02681102.2013.841629

van Dijk, J., Kalidien, S., & Choenni, S. (2018). Smart monitoring of the criminal justice system. *Government Information Quarterly, 35*(Supplement), S24–S32. doi:10.1016/j.giq.2015.11.005

van Rijnsoever, F. J. (2017). (I Can't Get No) Saturation: A simulation and guidelines for sample sizes in qualitative research. *PLoS ONE*, (7), e0181689.

doi:10.1371/journal.pone.0181689

VanScoy, A., & Evenstad, S. B. (2015). Interpretative phenomenological analysis for LIS research. *Records Management Journal, 71*(2), 338-357. doi:10.1108/JD-09-2013-0118

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly, 37*(1), 21-54.

Vincent, N. E., Higgs, J. L., & Pinsker, R. E. (2017). IT governance and the maturity of IT risk management practices. *Journal of Information Systems, 31*(1), 59-77. doi:10.2308/isys-51365

Vu , H. L., Khaw, K. K., & Tsong Yueh, C. (2015). A new approach for network vulnerability analysis. *Computer Journal*, *58*(4), 878-891. doi:10.1093/comjnl/bxt149

Wagner, M. (2016). The hard truth about hardware in cyber-security: it's more important. *Network Security*, *(12)*, 16-19. doi:10.1016/S1353-4858(16)30117-9

Walsh, P. F., & Miller, S. (2016). Rethinking 'five eyes' security intelligence collection policies and practice post Snowden. *Intelligence & National Security*, *31*(3), 345-368. doi:10.1080/02684527.2014.998436

Wang, D., Li, W., & Wang, P. (2018) Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks. *IEEE Transactions on Industrial Informatics, Industrial Informatics, IEEE Transactions on, IEEE Trans. Ind. Inf*, (9), 4081. doi:10.1109/TII.2018.2834351

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems*, 9225-35. doi:10.1016/j.dss.2016.09.013

Weidmann, N. B. (2015). A closer look at reporting bias in conflict event data. *American Journal of Political Sciences*, n.p. doi:10.1111/ajps.12196

Wheeler, A. J. A., & Mcelvaney, R. (2018). "Why would you want to do that work?" The positive impact on therapists of working with child victims of sexual abuse in Ireland: a thematic analysis. *Counselling Psychology Quarterly, 31*(4), 513–527. doi:10.1080/09515070.2017.1336077

White, G., Ekin, T., & Visinescu, L. (2017). Analysis of protective behavior and security incidents for home computers. *Journal of Computer Information Systems*, *57*(4), 353-363. doi:10.1080/08874417.2016.1232991

Willison, R., & Warkentin, M. (2013). Beyond deterrence: an expanded view of employee computer abuse. *MIS Quarterly, 37*(1):1e20.

Wu, F., Li, X., Sangaiah, A. K., Xu, L., Kumari, S., Wu, L., & Shen, J. (2018). A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. *Future Generation Computer Systems*, 82727-737. doi:10.1016/j.future.2017.08.042

Wu, T. F., Ganesan, K., Hu, Y. A., Wong, H. P., Wong, S., & Mitra, S. (2016). TPAD: Hardware trojan prevention and detection for trusted integrated circuits. *IEEE Transactions on Computer-Aided Design of Integrated Circuits & Systems*, *35*(4), 521-534. doi:10.1109/TCAD.2015.2474373

Xie, Q., & Hwang, L. (2019). Security enhancement of an anonymous roaming authentication scheme with two-factor security in smart city. *Neurocomputing*, *347*, 131–138. doi:10.1016/j.neucom.2019.03.020

Xu, M., & Han, W. (2019). An explainable password strength meter addon via textual pattern recognition. *Security & Communication Networks*, 1–10. doi:10.1155/2019/5184643

Yang, C., Zhang, J., Guo, J., Zheng, Y., Yang, L., & Ma, J. (2019). Fingerprint protected password authentication protocol. *Security & Communication Networks*, 1–12. doi:10.1155/2019/1694702

Yang, T., Ku, C., & Liu, M. (2016). An integrated system for information security management with the unified framework. *Journal of Risk Research, 19*(1), 21-41. doi:10.1080/13669877.2014.940593

Yevseiev, S., Kots, H., Minukhin, S., Korol, O., & Kholodkova, A. (2017). The development of the method of multifactor authentication based on hybrid cryptocode constructions on defective codes. *Eastern-European Journal of Enterprise Technologies*, *89*(9), 19-35. doi:10.15587/1729-4061.2017.109879

Yin, R. K. (2014). *Case study research design and methods* (5th ed.). Thousand Oaks, CA: Sage.

Yin, R. K. (2016). *Qualitative Research from Start to Finish* (2nd Ed.). New York, NY: The Guided Press

Yoo, C., Sanders, G. L., Rhee, C., & Choe, Y. (2014). The effect of deterrence policy in software piracy: cross-cultural analysis between Korea and Vietnam. *Information*

Development, 30(4), 342-357. doi:10.1177/0266666912465974

Yoon, J., Dunlap, S., Butts, J., Rice, M., & Ramsey, B. (2016). Evaluating the readiness of cyber first responders responsible for critical infrastructure protection. *International Journal on Critical Infrastructure Protection*, 1319-27. doi:10.1016/j.ijcip.2016.02.003

You, I., Ogiela, M. R., Woungang, I., & Yim, K. (2016). Innovative security technologies against insider threats and data leakage. *International Journal of Computer Mathematics*. 236-238. doi:10.1080/00207160.2015.1044784.

You, Y., Cho, I., & Lee, K. (2016). An advanced approach to security measurement system. *The Journal of Supercomputing 72* (9), 3443-3454. doi: 10.1007/s11227-015-1585-7

Young, W., & Leveson, N. G. (2014). An integrated approach to safety and security based on systems theory. *Communications of the ACM, 57*(2), 31-35. doi:10.1145/2556938

Yu, X., Wang, Z., Li, Y., Li, L., Zhu, W. T., & Song, L. (2017). EvoPass: Evolvable graphical password against shoulder-surfing attacks. Computers & Security, 70, 179–198. doi:10.1016/j.cose.2017.05.006

Zhang, H., Yao, D., Ramakrishnan, N., & Zhang, Z. (2016). Causality reasoning about network events for detecting stealthy malware activities. *Computers & Security*, 58180-198. doi:10.1016/j.cose.2016.01.002

Zhang, L., Tang, S., Chen, J., & Zhu, S. (2015). Two-factor remote authentication protocol with user anonymity based on elliptic curve cryptography. *Wireless*

Personal Communications, 81(1), 53-75. doi:10.1007/s11277-014-2117-0

Zhang, X., Kuchinke, L., Woud, M. L., Velten, J., & Margraf, J. (2017). Full length article: Survey method matters: Online/offline questionnaires and face-to-face or telephone interviews differ. *Computers in Human Behavio*r, 71172-180. doi:10.1016/j.chb.2017.02.006

Zheng, K., Cai, Z., Zhang, X., Wang, Z., & Yang, B. (2015). Algorithms to speedup pattern matching for network intrusion detection systems. *Computer Communications,* 6247-58. doi:10.1016/j.comcom.2015.02.00

Zhou, L., Chen, J., Zhang, Y., Su, C., & James, M. A. (2019). Security analysis and new models on the intelligent symmetric key encryption. *Computers & Security, 80,* 14–24. doi:10.1016/j.cose.2018.07.018

Zhu, Q., & Cen, C. (2017). A novel computer virus propagation model under security classification. *Discrete Dynamics in Nature & Society*, 1–11. doi:10.1155/2017/8609082

Zou, F., Zhang, S., Rao, W., & Yi, P. (2015). Detecting malware based on DNS graph mining. *International Journal of Distributed Sensor Networks*, 20151-12. doi:10.1155/2015/102687

Appendix: Interview Questions

1. What security strategies could be utilized to combat database threats posed by hackers?
2. How can external and insider threats compromise your organizational database system
3. What challenges do you have in addressing the security threats posed by cybercriminals or social engineers?
4. What technical strategies have you employed to protect database systems from data breaches?
5. What programs do you use to protect database systems from security vulnerabilities?
6. What measures do you take to mitigate risk in case of database compromise?
7. How does your experience in failures of technical and non-technical controls contribute to security breaches?
8. What additional information can you provide to assist me in understanding the phenomenon?