Exploring the Strategic Cybersecurity Defense Information Technology Managers Should Implement to Reduce Healthcare Data Breaches

Maurice Mawel
mauricemawel@yahoo.com
U.S. Department of State (DoS)
Washington, DC – U.S.

Samuel Sambasivam
Samuel.sambassivam@woodbury.edu
Computer Science Data Analytics
Woodbury University
Burbank, CA 91504

Abstract

The principal investigator (PI) conducted the research study to explore the strategic cybersecurity defense IT Managers should implement to reduce healthcare data breaches. The PI conducted a systematic literature review and selected articles that addressed healthcare data security breaches, information disclosure, cybersecurity in healthcare, and IT Managers' lack of leadership competence. Also, various annotations from contextual, seminal, grey, and recent literature were used to find the research problem: The strategic cybersecurity defense IT Managers should implement to reduce healthcare data breaches has not been established. The PI collected secondary data from the Office of Civil Rights (OCR)/Department of Health and Human Services (HHS). The analysis, results, and findings are provided below in Part 9. Nevertheless, the routine interaction during health information exchange (HIE) on an interoperable network and the behavior of care providers and third parties who use computers and mobile devices to exchange patient data is an opportunity for cybercriminals to install malware or launch a ransomware attack to exploit potential vulnerabilities whether to steal sensitive data or compromise the network systems. Therefore, strategic cyber defense or an innovative security model would mitigate the threat. An exploratory design is used, and an epistemological approach supports the research method and design. The study is significant, and it will contribute to the body of knowledge the PI suggested for future research and provide major recommendations.

Keywords: Health information exchange, Innovative security models, Interoperability, and Ransomware attack.

1. INTRODUCTION

The PI explores the strategic cybersecurity defense IT Managers should implement to reduce healthcare data breaches. Healthcare data and information improve the quality of care and safety. Medical data security is considerable because it becomes a fundamental challenge that necessitates establishing proactive strategic cyber defense aiming to secure healthcare data and minimize the occurrence of data breaches when the data is at rest or in motion (Offner et al., 2020). Saleem and Naveed (2020) concluded that the existing security technologies could not

meet many healthcare organizations' requirements or needs in preventing data breaches. One of the requirements is the association of different entities of an organization to create a framework for data breach mitigation strategies.

The healthcare industry collects, and stores highly sensitive and confidential data constantly exchanged between medical staff, patients, and third parties (Offner et al., 2020).
Human error is attackers' primary opportunity to compromise organizations and data breaches. Some human errors that lead to data breaches are social engineering, reusing passwords, storing plain-text passwords, ignoring intrusion warnings, failing to update software, and uploading sensitive data to the cloud (Saleem & Naveed, 2020).

However, the PI conducted a systematic literature review involving contextual, seminal, grey, and recent literature coupled with primary and secondary data related to prior studies—the study started by locating scholarly journal articles related to previous research on healthcare data breaches. Healthcare providers include doctors, clinicians, psychologists, dentists, pharmacists, surgeons, and nurses. Business associates or third parties are a health plan, including insurance companies, billing companies, electronic medical companies, and government programs like the Centers for Medicare and Medicaid Services (CMS). Therefore, cybersecurity and other security tools must be efficient or helpful in detecting, deterring, and identifying cyber threats and addressing security breaches quickly and systematically (Arockiasamy, 2021). The qualitative method and exploratory design were selected to help the PI examine the phenomenon, and the method is supported by the conceptual framework and its three sub-theories defined in the paper. The study will contribute to the body of knowledge and will benefit other researchers, practitioners, IT professionals, postgraduate students, many healthcare organizations, and non-healthcare organizations not only in the United States (U.S.) but in other countries.

2. RESEARCH PROBLEM

The problem to be studied is that the strategic cybersecurity defense IT Managers should implement to reduce healthcare data breaches have not been implemented (Sultana et al., 2020; Offner et al., 2020). Spanos and Angela found in 2016 that 37 related journal articles from 45 studies were related to healthcare data breaches. The two researchers analyzed that 75.6 percent of the event studies indicated data breaches have significant and adverse effects on organizations' strategic goals (Juma'h & Alnsour, 2020). Bourquard and Berler (2021) suggest that innovative solutions are needed in healthcare for secure interoperability and digital services. The Health Information Portability and Accountability (HIPAA) reported 642 data breaches as the most significant breach in 2020 by healthcare providers, healthcare clearinghouses, and other third parties associated with 25% record-breaking, which is more than 2019 (HIPAA Journal, 2021).

Security Managers in most healthcare organizations lack modern security tools to mitigate cyber risks that lead to data breaches. However, security awareness and training are provided to hospital employees (Legaspi, 2019). In 2014, a hacker group known as Deep Panda or Black Vine targeted Anthem (a healthcare insurance company) network system with malware and masqueraded on their Virtual Private Network (VPN). Attackers had privilege escalation, which led them to cause a healthcare data breach of 78.8 million patients' records (Saleem & Naveed, 2020).

3. THE RESEARCH QUESTION

The central research question is outlined here: What the strategic cybersecurity defense IT Managers implement to reduce healthcare data breaches should be? In addition, the PI used twelve probe questions related to the central guiding question:

1) What is the frequency of healthcare data breaches in a healthcare organization in the U.S.?
2) What are the most prevalent data security breach challenges of the last three years in a healthcare organization?
3) How many years of experience have IT managers implemented cybersecurity defense to secure healthcare data or prevent data breaches?
4) What strategies were not successful for securing healthcare data from security breaches?
5) How do IT leaders plan to develop an interprofessional collaboration in establishing a strategic cybersecurity defense across healthcare organizations in the U.S?
6) What mode of security training, formal or informal, to improve the security of EHRs

was provided during the past 12 months in a healthcare organization?
7) What model of cryptography algorithm is used to encrypt health data and enhance data security in a healthcare organization?
8) What successful security strategies do IT Managers use to protect healthcare data from security breaches?
9) What strategies were not successful for securing data from breaches?
10) What cloud service is used in healthcare organizations (SaaS, PaaS, IaaS, CLAaaS, DaaS, and more)?
11) What are the most significant risks to storing healthcare data in the cloud?
12) Is there a data security breach while using any of the cloud services?

The PI used the above questions listed to deduce the answers from the collected secondary data and to analyze the cleaned data.

4. LITERATURE SEARCH STRATEGIES

The research study identified relevant search engines and databases, such as Computer Science Database (ProQuest), ProQuest dissertations and theses, Google Scholar, ACM Digital Library, and Science Direct, from Colorado Technical University (CTU) Doctoral Library database and other online databases. Besides, the PI examined peer-reviews, journal articles, publications, books or electronic books, periodic magazines, and some dissertations during the literature review. Contextual, seminal, grey, and recent literature dating from 2016 to 2022 were examined and selected to raise the relevance and impact of the management and organization of the research study (Adams et al., 2016).

However, numerous safeguards are needed because many incidents of unauthorized data security breaches have been reported regularly in the Indian healthcare organization, which yields the urgency of establishing effective security mechanisms (Aljuaid & Parah, 2021). Keywords search focus on healthcare data breaches, cause of health data security breaches, cloud data security management, and solutions to a security breach were used with a Boolean expression. Furthermore, the PI expanded the search to healthcare organizations in the Washington Metropolitan area, including the Department of HHS with its various entities: HIPAA Journal, Office of Civil Rights (OCR), Office of the National Coordinator (ONC) for Health Information, which publish periodic Magazines or journals, HHS Blog, and News Release on their website https://www.hhs.gov/news. The department publishes reliable and valuable information related to healthcare and government-related issues, precisely healthcare information such as data security and privacy, COVID-19, and annual financial reports, and shares their archival data with its subscribers.

5. CONCEPTUAL FRAMEWORK

The research study aimed to explore the strategic cybersecurity defense IT Managers should implement to reduce data breaches in healthcare organizations in Washington metropolitan area. The research gap listed earlier was depicted from recent, contextual, grey, and seminal literature. The relationship between the three theories from the conceptual framework elicits interrelated behaviors. It demonstrates how IT Managers, covered entities, and third parties interact with patients' data, whereas a cybercriminal may exploit any potential vulnerability. The study problem was that the strategic cybersecurity defense IT Managers should implement to reduce healthcare data breaches has not been established. The conceptual framework supported the research study and defined the following three theories:

Routine Activity Theory (RAT)
These relationships reside in users' attitudes or routines when using computers or mobile devices to perform activities, access cloud healthcare data, and share EHRs. Some researchers have used RAT to study six cybercrimes or criminal behaviors and determined that the RAT elements showed varying results, although it presented clear indications for policy and crime prevention strategy (Cohen & Felson, 1979; Leukfeldt & Yar, 2016). Moreover, human error is associated with the routine and behavior of not creating a strong password, scanning their devices, or using anti-virus software. A lack of compliance with the security requirements might become an issue that may allow a cybercriminal to cause data breaches. The second cause of data breaches is employees' error, negligence, and voluntary disclosure of data (Swede et al., 2019).

Criminological Theory (CT)
Criminology theory explains the mystery of why crime occurs, and it allows us to consider the social context in which theories are formulated, published, and accepted as feasible (Lilly et al., 2018). The Identity Theft Resource Center (ITRC) report indicates data breaches happen the most through hacking, including ransomware, phishing, and other malware attacks (Swede et al., 2019). From 2010 to 2018, over 2,529 data

breaches affected 194,74 million patient's EHRs due to hacking (Hossain et al., 2019).

Game Theory for Security (GTS)

The theory deals with cybersecurity or data breach security issues and describes the attack landscape and decision-making process. Further, it designs an optimal controller for cyber-physical systems, including relevant countermeasures based on hardware and software security on a network with various dynamic defense mechanisms and opportunities in a healthcare organization (Zarreh et al., 2018). Cybercriminals exploit vulnerabilities in cloud computing or computer networking where the devices and communication channels may lack proper strategic security systems and security awareness training. Thus, this can enable threats to health information (Ondiege et al., 2017). Increased connectivity to existing computer networks has exposed medical devices to new cybersecurity vulnerabilities (Swede et al., 2019).

6. POPULATION AND DATA COLLECTION PROCEDURE

The study sample is a subset of the selected population; the estimated population comprises three different healthcare organizations within the Department of HHS. This organization and its entities store and publish reports on healthcare data breaches, cybersecurity incidents, and various information concerning the U.S. Government and public and private sectors. These entities work concomitantly with the Department of HHS or closely with hospitals, clinics, the Centre of Medicare and Medicaid Services (CMS), and the Centers for Disease Control and Prevention (CDC), located in the Washington Metropolitan area. According to Arockiasamy (2021), the population listed above contains a data breach portal that is the publicly available database that subscribers can access and download, although the IRB requires evidence of data collection permission to enhance transparency.

However, a pilot study was conducted to determine the feasibility of the study when the PI tried to proceed with semi-structured interviews. However, the result of this study persuaded the PI to immediately switch to secondary data collection rather than meeting participants to collect data. Ln (2017) explained that a pilot study is the first step of the entire research protocol and is often a smaller-sized study assisting in planning and modifying the main research study. The PI made these changes after sending emails to potential participants or making phone calls to explain the objective and goal of the research study; however, the PI received no feedback from ten IT leaders. In other words, their non-response or lack of communication obligated the PI to switch to a plan B, which was Not Human Subject Research (NHSR). Koczkodaj et al. (2019) explained that security rules established by HITECH and HIPAA stipulate the unsecured protected health information breach is the official Act term that requires, in some cases, care providers and third parties or covered entities to provide breach notification to the media.

The IRB approval authorized the PI to start data collection after obtaining site permission, email, and evidence of data use permission letter. The IRB committee regulates the research study processes by providing guidelines and assurance that no physical harm or psychological, social, or economic risk should alter the study before, during, and after the study endeavor (Legaspi, 2019). After contacting the IT Manager at the OCR for NHSR, the PI reiterated the data collection purpose and explained that there would be no risk of harm or exposure. EHRs, PHI, PII, or EMRs are targeted the most by hackers because they contain patient data and information, such as credit cards, financial information, name and address, telephone number, and more that can be sold in a dark market (Rivers, 2020). Still, safety, privacy, and confidentiality were ensured before, during, and after the study.

7. INSTRUMENTATION, TRANSCRIPTION, AND RETENTION

The PI used instruments during data collection, such as a Dell laptop computer with 1TB disk storage capacity and 8GB RAM and a Segregate External Hard drive to download and store secondary data. There was also an Apple iPhone 11 series to take images or photographs of relevant data or pages (that the computer could not download) that contained valuable information related to healthcare data breaches. During data collection, the environment and site were exempted from noise and distraction. At the end of data collection, the PI kept the data and instruments inside a locked bag on the car's trunk from the site to his residence to ensure security, confidentiality, and accuracy of the data collected. The length of collecting secondary data was about 60 minutes before noon. Data transcription took place at home—extracting relevant data or information from computer storage media and using handwriting to collect data from iPhone cameras. However, as the

HIPAA data retention policy recommends, the collected data has been saved inside one of my external hard drives for at least six years (archive).

8. STUDY SAMPLE AND ANALAYSIS OF SECONDARY DATA

The PI kept 85 kilobytes (KB) of healthcare data for analysis in a word document and excel spreadsheets that addressed data breaches and hacking incidents. Among the 85 KB, the PI extracted 845 records from the 65536 excel spreadsheet of data breaches and hacking IT incidents published by the OCR from 2019 to 2021. To be more explicit, the PI compiled excel spreadsheet data but extracted only 845 records of data breaches and hacking IT incidents that happened precisely from January 15, 2021, to December 21, 2021, in the Washington Metropolitan area: District of Columbia (DC), Virginia (VA), and Maryland (MD), and the rest of the word document data that was over 15KB, only 2KB of that data were analyzed or coded. A proposed data analysis model starts with transcription, data coding, categorizing, theming, and interpretation. During the data analysis and interpretation, bias and error were eliminated to ensure accuracy or reliability or to determine the trustworthiness.
The following figure describes the above coding process or data analysis procedure:

Interpretation-Focused Coding and Theming Strategies
The data analysis process necessitated using the interpretation-focused strategy highlighted above. After labeling the research question, searching for relevant information in the data, and assigning an anchor code to the relevant information, the PI moved on by grouping or sorting related codes. Furthermore, the PI used the same strategy for theming by looking at the high frequency of each code to finally interpret the associated themes that constitute the data and information obtained. These twelve probe questions or sub-questions listed in point 3, the research question was assigned to a definite anchor code to look for relevant data that answers the research question—seemingly a participant's response to an interview question.

9. RESULTS AND FINDINGS

After analyzing each anchor code and grouping themes based on their relationships, the PI combined and compiled the patterns to generate three main or top themes:

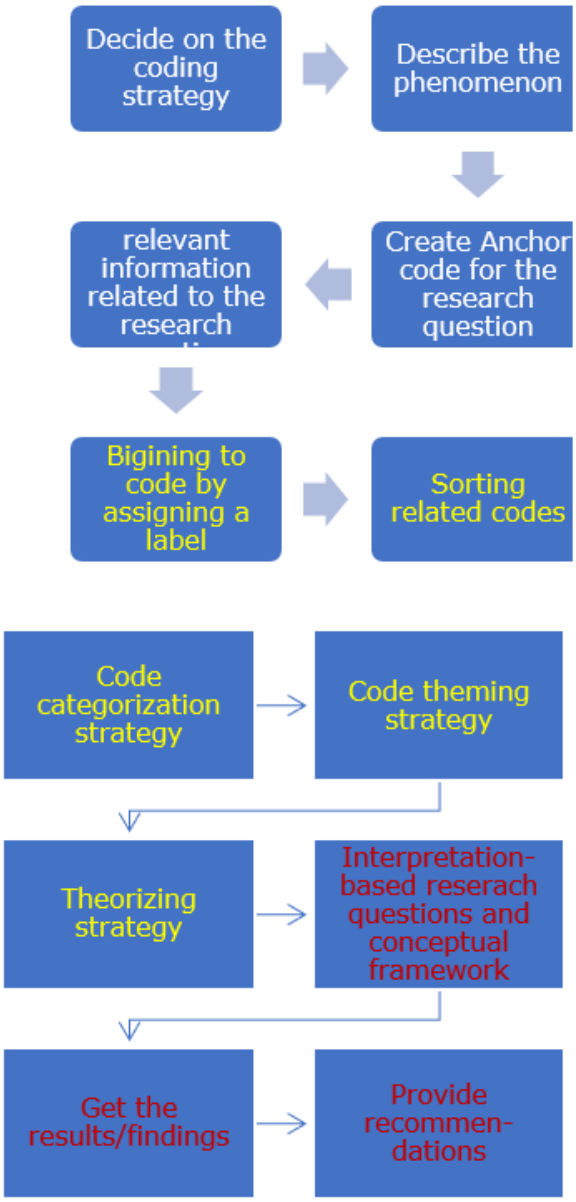

Figure 1: Understanding Data Coding, Analysis, and Interpretation

Top Theme 1
Corresponds to the lack of IT Managers' expertise or experience, and it appears 35 times.

Top Theme 2
Corresponds to third parties' involvement in HIE and appears 20 times.

Top Theme 3
Corresponds to major hacking/IT incidents and breaches appears 14 times.
Nevertheless, the implication of covered entities and business associates in accessing and sharing

EMRs or ePHI over the cloud or network is a root cause of hacking/IT incidents and the rise of data breaches. The PI found a lack of management expertise in establishing the strategic cybersecurity defense, and such weakness lures cyber-attackers to exploit vulnerabilities found during HEI. The PI used the triangulation approach by compiling the results generated from this analysis and OCR's annual report of data breaches and hacking IT incidents.

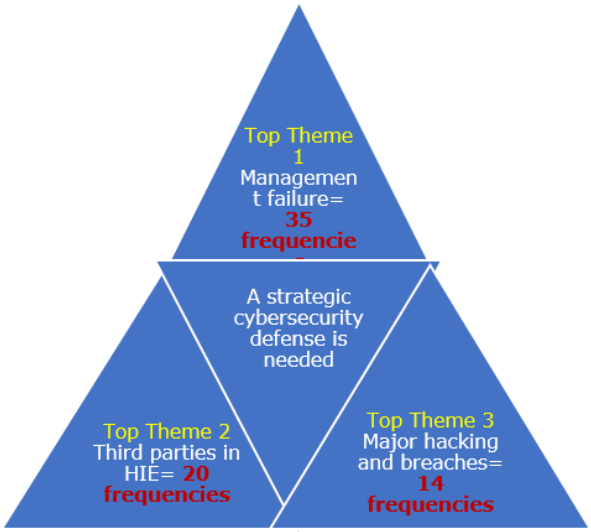

Figure 2: The Code frequency rates and three top themes

Therefore, the PI assumed that the results and findings were related to the conceptual framework and answered the research question based on the analysis. The analysis presented the following results: 73 codes and 69 frequencies, and IT Managers have failed to establish cybersecurity defense in an interoperable network. Furthermore, there is a relationship between the rise of healthcare data breach incidents and the involvement of covered entities and business associates in accessing and sharing EMRs or ePHI over the cloud or network. The frequency depends on each healthcare organization's security platform.

The PI coded the data manually, although doing so was time-consuming. Findings confirmed a lack of establishment of the strategic cybersecurity defense IT Managers should implement to reduce healthcare data breaches. The PI's coding strategy, known as interpretative-focused coding, sustained the interpretation of these codes and data. Still, qualitative data analysis, whether manual or with software tools, should support the researcher's efforts in presenting the results and findings that enhance trustworthiness or transparency (O'Kane et al., 2019).

10. FUTURE RESEARCH AND RECOMMENDATIONS

Further Research

The PI suggests a quantitative research method to investigate IT Managers' perception of interprofessional collaboration and continuous learning. Kidd et al. (2020) discussed that IT Security Engineering needs interprofessional skills to work collaboratively and negotiate the contributions of various disciplines while working on cybersecurity problems that require a multidisciplinary approach. Integrating knowledge and practices from multiple IT subject matter experts will enhance their perspective and ability to develop innovative solutions to fight against cyber criminals or threats. A second quantitative research method is suggested to explore third parties' level of education as they use computers to access health information.

Recommendations

According to Chigada and Madzinga (2021), the WHO research analysis indicates that cyber-attacks have increased quantitatively because research studies on cyber risks are still insufficient. Therefore, innovative security management practices are needed to solve cyber threats in the healthcare industry. As such, the PI recommends strategic cybersecurity defense to IT Managers and other practitioners; that is, IT Managers should strive to:

- Use modern or sophisticated tools to recognize threat actors.
- Categorize users into groups based on risk level and know the most attacked user.
- Ensure the security platform addresses use cases and compliance concerns.
- Enhance security awareness training and education on email phishing techniques, ransomware attacks, and social engineering because users generally represent a risk to any organization. Moreover, covered entities and third parties shall take periodic security awareness training-based information systems security courses.

11. CONCLUSION

The PI conducted the qualitative research study to explore the strategic cybersecurity defense IT Managers should implement to reduce healthcare data breaches. The question that was addressed

in the study was: What strategic cybersecurity defense IT Managers implement minimize healthcare data breaches should be? The PI collected and analyzed secondary data to answer the above central research question and twelve other probe questions. The findings provided a theoretical explanatory approach to the research problem and the contextual aspects associated with IT Managers' lack of expertise in implementing the strategic cybersecurity defense that should reduce healthcare data breaches. In addition, the PI analyzed that users' routine and behavior in accessing and sharing patients' healthcare data was found to be associated with cyber-attackers' exploitation of vulnerabilities in an interoperable network. The PI provided valuables recommendations and suggested further research studies in quantitative methods to investigate IT Managers' perception of interprofessional collaboration and continuous learning, and secondly to conduct another quantitative research method to explore third parties' level of education as they use computers to access health information.

12. ACKNOWLEDGMENTS

I dedicate this research study and doctorate to three people— God with his Son Jesus-Christ, my late mother Francisca Ngo Bikai, and my nuclear family. My mother is the inspiration for my education; she took care of me after my dad's passing in 1965; sacrificed herself to enroll me in school in a small city of Cameroon known as Eseka. The Almighty God, through Jesus Christ, opened a door of opportunities by taking me from my original country Cameroon to the United States. Also, they supported me by answering my prayers during the entire doctoral journey and achieving this goal. Lastly, I will not forget my wife Therese-Desiree, my daughter Elodie, and my three sons: Rene, James, and Nathaniel. They motivated me both intrinsically and extrinsically, although they sometimes worried about my long-standing and intermittent confinement in the study room. However, they did not stop showing me love, a positive mood, or a successful mindset. I will also give a big thanks to all my instructors from CTU with a special bonus to Dr. Sambasivam for making me a great man through this doctoral journey.

13. REFERENCES

Adams, R. J., Smart, P., & Huff, A. S. (2016). Shades of grey: Guidelines for working with the grey literature in systematic reviews for management and organizational studies. *International Journal Management Reviews*. https://doi.org/10.1111/ijmr.12102

Aljuaid, H., & Parah, S. (2021). Secure patient data transfer using information embedding and hyperchaos. *Sensor Networks and IoT for E-health Applications 21(1*), 282. https://doi.org/10.3390/s21010282

Arockiasamy, A. A. (2021). *Impact of information breaches on health care records* (Publication No 28318026) [Doctoral dissertation, Walden University]. ProQuest Dissertations and Theses Global.

Bourquard, K., & Berler, A. (2021). Health information exchange: The overarching role of integrating the health enterprise (IHE). *Introduction to Nursing Informatics*. https://doi.org/10.1007/978-03-030-58740-6_5

Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management 23*(1). https://doi.org/10.4102/sajim.v23i1.1277

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activityapproach. *American Sociological Review 44(*4), 588-608. https://www.jstor.org/stable/2094589

HIPAA Journal. (2021, January 19). 2020 Healthcare data breach report: 25% Increase in breaches in 2020. *HIPAA Journal*. https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/

Hossain, M. M., Hong, A. Y., & Symp, A. (2019). Trends and characteristics of protected health information breaches in the United States. *AMIA Annual Symposium Proceedings Archives*. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7153056/

Juma'h, A. H., & Alnsour, Y. (2020). The effect of data breaches on company performance. *International Journal of Accounting and Information Management 28(*2), 275-301. https://doi.org/10.1108/IJAIM-01-2019-0006

Kidd, J., Kaipa, K., Sacks, S., Ringleb, S., Pazos, P., Gutierrez, K., Ayala, M. O., & de Souza Almeida, M. L. (2020). What do undergraduate engineering students and pre-service teachers learn by collaborating and teaching engineers and coding through robotics? *Asee's Virtual Conference at Home with Engineering Education*. https://par.nsf.gov/servlets/purl/10189269

Koczkodaj, W. W., Masiak, J., Mazurek, M., Strzalka, D., & Zabrodskii, P. F. (2019). Massive health record breaches evidenced by the office for civil rights data. *Iranian Journal of Public Health* 48(2), 278-288. https://pubmed.ncbi.nlm.nih.gov/31205882/

Legaspi, J. (2019). *Exploring the cybersecurity measures healthcare managers use to reduce patient endangerment resulting from backdoor intrusions into medical devices* (Publication No 13813275) [Doctorate dissertations, Colorado Technical University]. ProQuest Dissertations and Theses Global.

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

Lilly, J. R., Cullen, F. T., & Ball, R. A. (2018). *Criminological theory: Context and consequences*. (7th, Ed.). Sages Publishing.

Ln, Y. (2017). Introduction of a pilot study. *Korean Journal of Anesthesiology 70*(6), 601-605. https://doi.org/10.4097/kjae.2017.70.6.601

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

O'Kane, P., Smith, A., & Lerman, P. M. (2019). Building transparency and trustworthiness in inductive research through computer-aided qualitative data analysis software. *RMD Academy of Management.* https://doi.org/10.1177/1094428119865016

Ondiege, B., Clarke, M., & Mapp, G. (2017). Exploring a new security framework for remote patient monitoring devices. *Computers MDPI, 6(1*), 1-13. https://doi.org/10.3390/computers6010011

Rivers, L. (2020). *Strategies for reducing the risk of data breach within the Internet cloud* (Publication No 28264644) [Doctorate dissertations, Walden University]. ProQuest Dissertations and Theses Global

Saleem, H., & Naveed, M. (2020). Sok: Anatomy of data breaches. *Proceedings on Privacy Enhancing Technologies 2020(*4), 153-174. https://doi.org/10.2478/popets-2020-0067

Sultana, M., Hossain, A., Laila, F., Taher, A. K., & Islam, N. M. (2020). Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology. *BMC Medical Informatics & Decision Making*. https://doi.org/10.1186/s12911-020-01275-y

Swede, M. I., Scovetta, V., & Eugene-Colin, M. (2019). Protecting patient data is the new scope of practice: A recommended cybersecurity curricula for healthcare students to prepare for this challenge. *Journal of Allied Health, 48(*2), 148-156. https://www.ingentaconnect.com/content/asahp/jah;jsessionid=f6mw6pmganap.x-ic-live-01

Zarreh, A., Saygin, C., Wan, H., Lee, Y., & Bracho, A. (2018). A game theory-based cybersecurity assessment model for advanced manufacturing systems. *Procedia Manufacturing 26(*1), 1255-1264. https://doi.org/10.1016/j.promfg.2018.07.162