12-11-2024

Successful Strategies Used By Health Care Business Managers to Reduce Data Breaches

Amber Branson Rubis
Walden University

Walden University

College of Management and Human Potential

This is to certify that the doctoral study by

Amber Branson

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. Kim Critchlow, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Jodine Burchell, Committee Member, Doctor of Business Administration Faculty

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

Walden University
2024

Abstract

Successful Strategies Used By Health Care Business Managers to Reduce Data Breaches

by

Amber Branson Rubis

M.B.A., Louisiana State University, 2021

B.S., University of Tennessee, 2020

Research Project Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

December 2024

Abstract

Ineffective strategies to reduce data breaches in healthcare organizations can harm patient safety, erode trust, and jeopardize financial stability. Healthcare managers Healthcare managers must implement effective strategies to protect their organization's reputation and ensure long-term business stability. Grounded in protection motivation theory (PMT), the purpose of this qualitative pragmatic inquiry was to explore strategies healthcare business managers used to reduce data breaches and sustain profitability. The participants were six healthcare business managers who had successfully implemented strategies to reduce data breaches and sustain profitability. Data were collected using semistructured interviews and public records. Using thematic analysis, four themes were identified: (a) coping appraisal-response efficacy, (b) response cost-effort, (c) threat appraisal-vulnerability, and (d) protection motivation-intent to act. A key recommendation is for healthcare business managers to embrace and use innovative technologies and advanced security measures, such as AI-driven threat detection systems, a proactive organizational culture, and continuous training programs, to reduce security risks and data breaches. The implications of positive social change include the potential to improve patient data protection, build trust, mitigate the economic impacts of data breaches, and empower healthcare leaders to create safer, more reliable environments while controlling healthcare costs.

Successful Strategies Used By Health Care Business Managers to Reduce Data Breaches

by

Amber Branson Rubis

MBA, Louisiana State University, 2021

B.S., University of Tennessee, 2020

Research Project Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

December 2024

Dedication

I dedicate this work to Our Lord and Savior Jesus Christ, the Heavenly Father, and the Holy Spirit. Your guidance and grace have been my foundation.

I want to express my deepest gratitude to my family: my father, Ronald Lee William Branson; my mother, Tina Lynn Branson; my sister, Heidi Kathryn Turner, and her husband, Larry Shane Turner; and my brothers, Lee William Branson and Nicholas Andrew Branson. To my nieces, Elizabeth (Buffy) Lehman and Sophia Branson Carter, your futures have been a source of inspiration throughout this journey.

I also honor the memory of my beloved grandparents: my mother's parents, Howard Elmer Miller and Ruth Arlene Faisal, and my father's parents, Winifred Katherine Branson and Orville Branson. I extend this dedication to my mother's sister, Susan Christine Hickman, and her deceased sister, Stephanie Ann Beavers. I also recognize my father's sisters, Teresa Sue Smith, Marilyn Jean Eulette, Regina May Cline, and his deceased sister, Carolyn Annette Woodruff. Your lives and legacies continue to inspire me.

Finally, to all the Luddites seeking better strategies—this is for you.

Acknowledgments

I would like to acknowledge my chair, Dr. Kim Critchlow and second committee member Dr. Jodine Burchell for your invaluable guidance and expertise on my doctoral journey.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Project

Background of the Problem

Data breaches are destructive to a health care organizations. In the United States, data breaches in health care are the highest in the world for 12 years (IBM, 2023). Health care data breaches can lead to reduced quality of care, with fatal consequences for patients (Seh et al., 2020). The average global cost of a data breach is $4.88 million and 70% of breached companies reported that the breach significantly impacted their operations (IBM, 2023). In previous studies, researchers focused on information technology infrastructure knowledge expertise for organizations to protect themselves from cybersecurity incidents (Hathaliya & Tanwar, 2020). Shahbaznezhad et al. (2019) demonstrate that security strategies implemented to employees without incorporating dynamic security training have slight improvement. The general problem is that some business managers lacking successful strategies to reduce data breaches in their organization impacts performance and profitability.

Business Problem Focus and Project Purpose

The specific business problem is that some health care business managers lack successful strategies to reduce data breaches and sustain profitability. Therefore the purpose of this qualitative pragmatic inquiry study is to identify and explore successful strategies some health care business managers use to reduce data breaches and sustain profitability

The targeted population consisted of six purposefully sampled health care business managers who have effective strategies to reduce data breaches and sustain profitability. Data sources for this project consisted of (a) semistructured interviews; (b) public data, such as publicly disseminated reports and public websites; (c) literature, such as books, peer-reviewed articles, and other bodies of written knowledge that communicate substantive research findings about practices that are relevant to the researcher's topic. The conceptual framework for this study includes protective motivation theory (PMT), which was developed by Rogers (1975). PMT describes how threats within their environment influence an individual's behavior.

Research Question

What successful strategies do some health care business managers use to reduce data breaches and sustain profitability?

Assumptions and Limitations

Assumptions

In this study, assumptions comprise statements that are assumed to be true (Durkin et al., 2020). I identified two assumptions in this study. The first assumption is that the participants interviewed would be truthful when answering the interview questions. The second assumption is that the participants, being health care business managers, represent the population faced with the challenges of this study and have employed successful strategies to address these issues. I validated these assumptions during the interview process and throughout the study.

Limitations

Ross and Bibler Zaidi (2019) defined limitations as uncontrollable conditions in a study that restrict the research outcomes. First, this qualitative pragmatic inquiry study includes only the factors involving health care business managers and their strategies to reduce data breaches and not all business managers. Second, healthcare business managers in a major hospital network may use techniques different from those of smaller companies. Third, the limitations associated with this study reside with the participant's potential lack of understanding, knowledge of their organization's effort to mitigate data breaches, or willingness to discuss them openly. As the time of employment and value of experiences differ, the participants may show discrepancies based on their perceptions or valuation of their organization's efforts to improve, which could lessen the strength of my findings. Work experience may also cause disparities as new managers' unfamiliarity with historical efforts may impair the implementation process of new strategies.

Transition

In Section 1, I defined the background of the problem and the problem statement. In this overview, I covered the purpose of the study, the research question, the assumptions, and the limitations of this study. In Section 2, I will review the professional and academic literature and identify the conceptual framework of the theory and its supporting theories. As part of the literature review, I researched articles on preventing and mitigating data breaches in health care organizations to identify themes and strategies included in previous steps on my research topic. In Section 3 of this study, I will review the literature and research project methodology, nature of the project, population and data sampling, ethical considerations, data organization analysis, reliability and validity, data saturation, and a transition into the conclusions of the proposed study. In Section 4, I will cover my research findings, identify themes and strategies, and make recommendations for health care business managers and other researchers as they search for methods that will assist them in mitigating security breaches and phishing attacks. I will also cover my reflections on my study.

Section 2: The Literature Review

A Review of the Professional and Academic Literature

Literature Review Opening Narrative

The health care industry faces a growing number of electronic health records (EHR) data breaches, a significant concern for health care organizations, physicians, and patients. According to Yeo and Banfield (2022), the costs of data breaches in the health care sector are the highest among all industries. While the adoption of EHR has improved patient care by providing real-time information, the increasing number of cyber-attacks on health care systems has raised concerns. Karambelas (2020) emphasized confidentiality, integrity, and availability of EHRs to maintain high-quality patient care.

A survey conducted by Ponemon Institute in 2023 involved 641 IT and I.T. security practitioners working in health care organizations. These practitioners were responsible for various cybersecurity strategies, such as setting IT cybersecurity priorities, managing budgets, and choosing vendors and contractors. According to the survey, 89% of the organizations experienced cyberattacks in the past 12 months. This section thoroughly explores scholarly literature published in the last 5 years to investigate data breaches of EHRs within the health care sector. This section begins with a brief statement of the problem, followed by an explanation of the research's purpose and the search technique used in the study. The following section discusses the conceptual framework used in the research study. According to Daniel and Wald (2019), the conceptual framework consists of a cohesive and integrated set of ideas, hypotheses, and principles. The conceptual framework model explains the relationship between the topic and how the framework would contribute to reducing data breaches in the health care industry. In this study, I used the PMT as my conceptual framework. While exploring the framework, I reviewed both current and historical scholarly literature on EHR data breaches. The section concludes with an analysis of the literature review and a conclusion. My search strategy involved using five databases to search for peer-reviewed journal articles related to EHR data breaches in health care systems. Specifically, I searched the following databases: ABI/Inform Global (ProQuest), ACM. Digital Library, Google Scholar, EEE/IET Electronic Library,ABI/Inform Global (ProQuest), and Google Scholar. Key search words used were: *Electronic health record data breach, Covered entities' data breaches, Health care cyber-attacks, Cybersecurity in health care sectors, Health care data loss, EHR data breaches,* and *Hacking incidents in health care.*

The search resulted in over 5,000 records. The next step was to filter the date range, ensuring that only articles written within the last 5 years were included in the review. After that, the next step was to choose a peer-reviewed article and access the full text. By using the advanced search function with the terms "health care system data breaches" and "qualitative study," the results were further narrowed down to the health care sector. The literature review comprised 69 peer-reviewed references. Of these, six references (9%) were published before 2019, while the remaining 63 (91%) were published after 2019. I accessed peer-reviewed scholarly articles published between 2019 and 2024 through the Walden University Library, ensuring their relevance to this study. Table 1 provides the article count for the literature review.

Table 1

Research References Breakdown

	Total sources	Peer reviewed	Non-peer reviewed	< 5 years	> 5 years
Journal articles	69	69	0	63	6
Percentage	100%	100.00%	00.00%	91.3%	8.69%

Application to the Applied Business Problem

My study's problem was identifying successful strategies used by healthcare business managers to reduce data breeches and sustain profitability.

Protection Motivation Theory (PMT)

In my research study, I used the PMT developed by Rogers in 1975 as the lens through which to view the project. According to Rogers (1975), PMT explains how an individual's motivation to protect themselves arises from environmental threats. The theory is concerned with avoiding maladaptive behaviors and is associated with an increased probability of engaging in adaptive solutions or recommendations. Previous research studies have shown that human error or user behavior is the leading cause of data breaches.

PMT consists of threat appraisal and coping appraisal. The threat appraisal component includes perceived severity, susceptibility, and reward, while the coping appraisal comprises response efficacy, self-efficacy, and response cost. Van Bavel et al. (2019) pointed out that when faced with a threat, an individual evaluates the threat and means of response before deciding whether to engage in specific protective behaviors.

A coping message encourages users to reduce their risk exposure when facing a threat. In contrast, a threat appeal emphasizes the potential negative consequences of not taking action to reduce the perceived threat. Xiao et al. (2021) explained that response efficacy, response costs, and self-efficacy form the basis of coping appraisals. The danger and the coping message increased secure behavior, but the coping message significantly improved users' secure behavior. Changing employee behavior through awareness training, rewarding, and safe behavior could help reduce cybersecurity incidents (Wang et al., 2020).

The PMT is relevant to and closely aligned with the research topic. Human error dramatically impacts the success of cyberattacks, so a cybersecurity strategy should focus on promoting secure behaviors among individuals. The PMT offers valuable insights into what motivates people to protect themselves online. Recent PMT research by Bayl-Smith et al. (2021) has highlighted the significance of the coping appraiser in cybersecurity.

Studies have revealed that employee negligence and errors are the leading causes of health care data breaches, making the human element of an organization's workforce the most susceptible part of cybersecurity. Employees serve as the first line of defense for cybersecurity and are crucial to managing enterprise information security. Encouraging their compliance with information security standards in the digital age is essential for safe and effective operations. Enterprises can enhance the impact of their security awareness programs by regularly conducting cybersecurity awareness training and information security communication sessions.

Seven factors influence employees' willingness to comply with an information security system: response costs, response efficacy, perceived severity, perceived susceptibility, rewards, self-efficacy, and social influence. W. Li et al. (2022) suggested that rewards, self-efficacy, and response costs are the core conditions with the highest probability of occurrence in each pathway. With the health care industry undergoing digital transformation, information systems and information security play a crucial role in daily operations. Organizations now develop and communicate information security policies to guide employees in navigating the digital landscape.

Research by Kuppusamy et al. (2020) has revealed that employees often fail to adhere to these policies. Employee negligence, errors, and noncompliance with security measures are the primary reasons behind data breaches (Kuppusamy et al., 2020). Threat and coping appraisals rooted in the PMT can help predict users' protective behaviors. When employees neglect security policies, it can result in data breaches involving unauthorized access to confidential or sensitive information, such as personal health information (PHI) and medical records. To uphold the confidentiality, integrity, and availability of data, information system users must be aware of the threats posed by modern technology and be prepared to take preventive measures against cyberattacks. The PMT can aid health care information system users in enhancing their cybersecurity resilience. Given the health care industry's shift towards digital processes, EHR systems are crucial for collecting, storing, and sharing patient-sensitive data. Ali et al. (2021) pointed out a significant risk of unauthorized access, disruption, modification, corruption, or destruction of this data.

Improving communication with users about the severity, likelihood, and effectiveness of responses to information security threats is essential to enhance cybersecurity efficiency in health care organizations. According to Sulaiman et al. (2022), the PMT can improve human behavior when dealing with security threats.

Despite solid security measures, humans remain the biggest threat to an organization's information system.

Previous research has indicated that the human element plays a significant role in data breaches. Exploiting human weaknesses has increased the risk of cyber incidents, highlighting the need for a more secure, awareness-based culture to encourage compliance. The likelihood of cyber incidents has increased in recent years, making the human aspect increasingly crucial in ensuring organizational data security and preventing data breaches, according to Andronache (2021). Previous research has not addressed the importance of fostering a cyber-aware culture in organizations to reduce the human element associated with data breaches.

In PMT theory, threat appraisal and coping appraisal are two distinct pathways. Threat appraisal assesses an individual's perception of the risk of certain behaviors, while coping appraisal considers the individual's ability to deal with the threat. Examples of threat appraisal include perceived vulnerability and severity. Manoharan et al. (2022) stated that coping appraisal includes response cost and self-efficacy.

Users need to understand the likelihood and potential severity of computer attacks, including ransomware attacks, to take preventive measures to mitigate them. Health care information security professionals can use the PMT to assess whether an organization effectively promotes cybersecurity measures among users. This theory can help health care cybersecurity managers implement a robust cybersecurity awareness program. Organizations can improve cybersecurity effectiveness by better motivating users and communicating the severity of threats, the likelihood of attacks, and the effectiveness of the response. However, behavioral change requires more than just providing knowledge about risks and reactive behaviors; individuals must also understand and apply the advice received. Additionally, according to Moustafa et al. (2021), individuals must exhibit motivation and willingness to engage in cybersecurity actions, which requires changes to their attitudes and intentions.

The PMT explores an individual's thoughts when facing a threat. When analyzing behavior, the theory considers motivation, probability, severity, vulnerability, response efficacy, self-efficacy, response cost, and reward. According to Andronache (2021), this theory helps determine the extent to which threat perception results in a favorable or unfavorable response. Additionally, Ali et al. (2021) state that PMT has proven effective in ensuring employee compliance with information security policies and defensive actions when confronted with a threat.

According to research by Marikyan and Papagiannidis (2023), PMT can be understood in information security using the example of a malware threat. When a malware threat emerges, users first assess whether their computers are vulnerable to infection (perceived vulnerability) and evaluate the severity of the virus to their system (perceived severity). They then consider whether their system is immune or susceptible to the virus (self-efficacy), the effort required to use protective software, and the effectiveness of virus control software in recognizing and eliminating malware (response cost). Research by Mou et al. (2022) suggested that threat and coping assessments predict the likelihood of individuals using malware protection software.

Security awareness programs should consider cultural factors when evaluating cognitive behavioral reactions PMT and conformance (institutional theory) in the context of information technology to prepare an organization for resilience better. Organizational culture varies and can encompass several layers, from prescriptive regulations to ideal behaviors. According to Andronache (2021), understanding that norms, behaviors, attitudes, and beliefs can holistically support an organization's performance can help organizations broaden their approach to risk mitigation.

Using the PMT provides valuable insights into why computer users may fail to take preventative measures, such as opening email attachments from unknown senders without verification and not adhering to company security policies and standards. Individuals' behaviors are influenced by their adaptability, which is evaluated based on their perception of potential benefits, the magnitude and susceptibility of the threat they face, and the efficacy of their response to the costs associated with their coping mechanism. A recent study found a strong correlation between threat-related traits, such as self-efficacy and coping beliefs, and adaptive reactions (Lemay et al., 2020).

To ensure that users take preventative measures, the information security risks presented to them must be distinct and easily relatable. Employees might hesitate to take preventive action despite being aware of computer security risks unless they are convinced that the risk is substantial, highly likely to occur, and might lead to specific types of damage. Regular communication can improve users' information security awareness and motivate behavior change. Studies on fear appeals have focused primarily on how fear-inducing communication influences behavior, leading researchers to develop the PMT. PMT researchers have argued that human behavior is determined through cost-benefit analysis, focusing on how fear-inducing communication influences behavior. T. Smit et al. (2021) noted that PMT argues that individuals assess their behavior by analyzing the costs and benefits of a particular action and weighing the associated risks against the expenses of attempting to avoid or mitigate them.

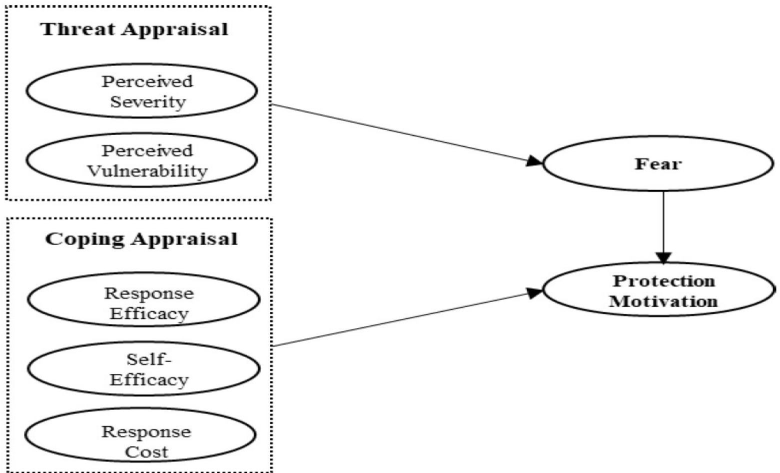
The PMT influences employees' responses to phishing attacks. According to Rogers (1975), PMT emphasizes that increasing people's awareness of potential threats makes them more fearful, leading to a greater likelihood of taking defensive actions. Additionally, Kam et al. (2020) suggested that a security-conscious organizational environment motivates employees to protect the organization's information assets by diligently adhering to information security policies. The organization's culture substantially impacts employees' compliance with security policies and standards.

Potential Themes and Phenomena

To understand how people behave and cope during stressful situations, the PMT has been used to emphasize the intrinsic and extrinsic factors that can lead to motivation and performance of the desired behavior. This understanding is expected to help formulate precisely tailored persuasive communication. The PMT framework involves threat appraisal and coping appraisal as the multidimensional determinants of motivation (see Figure 1).

Figure 1

PMT Model for Preventing Data Breaches



Note. Original Adapted from "A Test of PMT in the Information Security Literature: A Meta-Analytic Structural Equation Modeling Approach," by J. Mou, J. Cohen, A. Bhattacherjee, and J. Kim, 2022, *Journal of the Association for Information Systems, 23*(1), (https://doi.org/10.17705/1jais.00723).

Threat appraisal is the combination of perceived severity (perceptions regarding the Degree of harm) and perceived vulnerability (perceptions regarding the chance that one will experience harm) regarding the situation, excluding the perceived rewards (positive aspects) of the problem. A coping appraisal can be experienced as the combination of response efficacy (belief in the effectiveness of the recommended behavior in removing or preventing possible harm) and self-efficacy (the belief that one can successfully enact the recommended behavior). Subtracting the response costs (the perceived or actualized costs associated with the practice of the recommended behavior), these constructs intrinsic to the model ultimately lead to a protection motivation to perform adaptive responses. However, building on the experiences gathered in the research of perceived vulnerability and perceived severity, along with coping appraisal of protective behaviors regarding response efficacy and self-efficacy, have been presumed to be the significant determinants of security breach training. PMT has also been conceptually proposed in my current study that the practice of other preventive behaviors influences the practice of one particular behavior. Factors beyond these constructs may also affect the recommended preventive behaviors, e.g., occupation, education, knowledge, and personal experiences. Social media also has immense motivational value when the publicity has been highly negative regarding the security aspects of the organization.

To understand the dynamics of these factors in practicing preventive behaviors, three key themes emerged from the review of the literature: (theme 1) cybersecurity preparedness, (theme 2) development of coping appraisals, and (theme 3) changing employee behavior that promotes safety and security to help reduce cybersecurity incidents. Researchers of other studies have identified and measured the preventive practices and analyzed the determinants of these practices among security managers (Ajzen, 1991; IBM, 2023). In this current study, I used the PMT to explain why people engage in illegal and unsafe practices and offer suggestions for changing these behaviors through precise risk communication strategies. Risk communication and related perceptions as a basis for the desired behavioral change have not been studied adequately, especially in health care systems. The current research aimed to identify and evaluate the strategies that health care business managers use in the association between the practice of the selected preventive behaviors and threat perceptions, response efficacy, and self-efficacy to successfully reduce data breaches to sustain an organization's profitability.

Six key strategies emerged from the literature review: the threat appraisal component included perceived severity, susceptibility, and reward, while the coping appraisal comprised response efficacy, self-efficacy, and response cost. Surprisingly, the third theme discussed in the literature review covered changing employee behavior that promotes safety and security to help reduce cybersecurity incidents, consistent with the PMT conceptual framework. I will carefully evaluate this information from the literature review with my findings after completing the semistructured, open-ended interviews with my participants.

Hacking

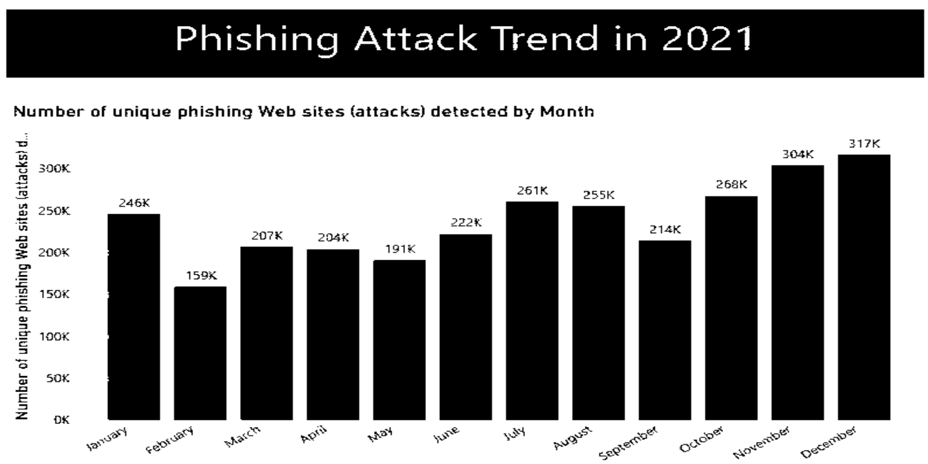
Hacking incidents encompass all cyber-attack methods used to gain unauthorized access to sensitive data, including electronic health records (EHR), electronic medical records (EMR), personally identifiable information (PII), personal health information (PHI), electronic personal health inforaiton (ePHI), medical health records (MHR), or credit card information. As defined by Fox and Holt (2020), computer hacking involves using specialized technological knowledge to gain unauthorized access and retrieve sensitive information from computer systems. The following section explores the most common hacking attacks that lead to data breaches.

Phishing

Phishing serves as a precursor to cyber-attacks, with email being the most commonly used medium for phishing. Attackers create fictitious email accounts to send deceptive emails to victims, deceiving them into taking action. Email is a widely used business application among end users. Still, its popularity also brings several risks, as cybercriminals frequently utilize emails to launch various cyber-attacks through spam, phishing, and malware distribution (Alohali et al., 2018). Phishing attacks are on the rise because the incentives for cybercriminals to use deceptive email for cybercrime are low-cost and require minimal effort from the perpetrators. Data from the anti-phishing group indicate an increase in the number of phishing websites, as depicted in Figure 2 below.

Figure 2

APWG Phishing Attack Trend 2021



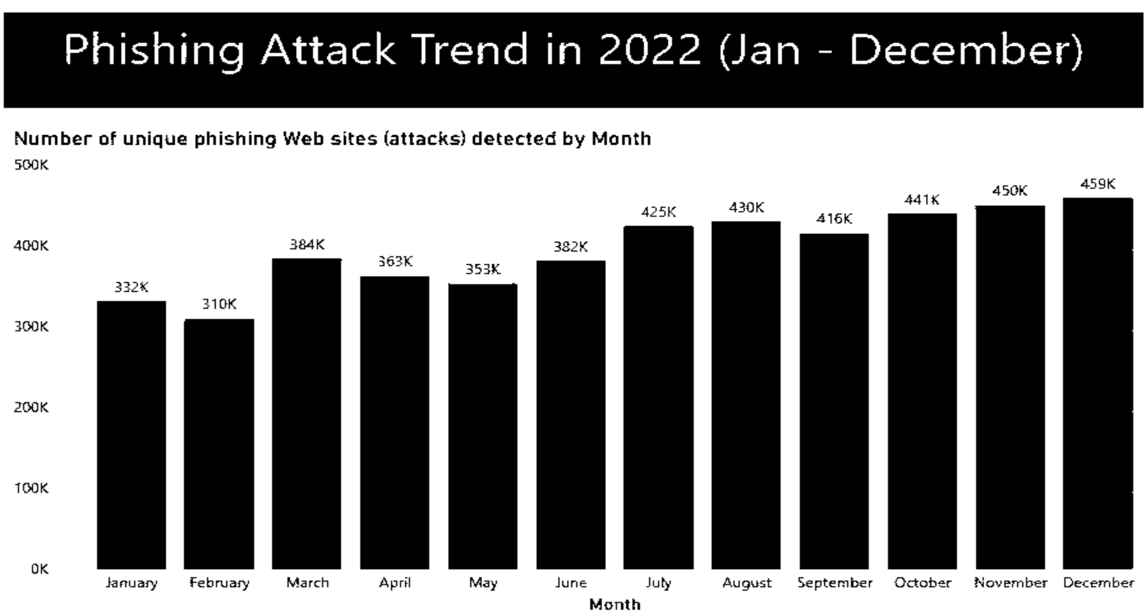
Note. The Phishing Attack Trend in 2021 from the Anti-Phishing Working Group (APWG, 2022a).

The Phishing Attack Trend in 2021 shows an increase in unique phishing websites compared to the previous year. According to the data in Figure 2, the number of unique phishing attack websites detected rose from 199k in December to 246k in January 2021. By December 2021, the number had increased to 317k. APWG (2022a) defines phishing as a crime that uses technological and social engineering deception to steal customers' financial accounts and PII. Phishers often use social engineering tactics, such as creating fictitious email accounts and messages, to deceive unsuspecting victims into believing they are interacting with a trustworthy entity.

Attackers frequently adjust their phishing campaigns to align with current events to maximize their impact. Russian hackers, for instance, used phishing emails to spread misinformation after the announcement of the 2016 U.S. presidential election results (Desouza et al., 2020). Their strategy involved sending emails from fabricated Harvard University email accounts, which exacerbated the sense of conspiracy surrounding the event. Phishing attacks can be sophisticated and well-planned, posing serious threats to the target and offering significant financial gain for the perpetrators. The number of unique phishing websites fluctuates monthly depending on world events, as illustrated in Figure 3.

Figure 3

APWG Phishing Attack Trend 2022



Note: The Phishing Attack Trend Chart 2022 from the Anti-Phishing Working Group (APWG, 2022b).

The data indicate that December had the highest number of phishing attacks. Phishing remains the preferred method for hackers to infiltrate networks due to its low cost and high returns for cybercriminals. Figure 3 illustrates that unique phishing websites increased to 459k in December 2022. This pattern suggests that phishing will continue to threaten organizations of all sizes seriously. Phishing is a common method cybercriminals use to hack into computer systems and create backdoors for further attacks (APWG, 2022b).

The percentage of employees who click on phishing emails has remained relatively stable at 2.9%, which is significant enough to incentivize criminals to persist in using this method (DeJonckheere & Vaughn, 2019). Phishing attacks are a growing concern in the health care sector. Hacking through email is cost-effective for cybercriminals, and the return on investment is high because it requires less effort.

Users and employees often rely on antivirus or anti-phishing software, providing them a false sense of security. Trust in technology becomes crucial when people find themselves in real cyber threats and must rely on technology. Trust in technology, similar to trust in people, is formed based on the perception of its attributes (Jalali et al., 2020).

Ransomware

Ransomware is a type of malware that uses blackmail to extort its victims. The term “ransomware” refers to a ransom note that asks the victim to pay a sum of money (ransom) to regain access to their data or device or for the attacker not to reveal the victim’s embarrassing or compromising information. Attackers typically spread ransomware via deceptive email attachments, infected software apps, external storage devices, or compromised websites (Hull et al., 2019). Ransomware is becoming more complicated, destructive, and widespread. Ready-to-go Ransomware as a Service (RaaS) has given even inexperienced attackers the tools they need to launch successful attacks (Kapoor et al., 2021).

As gatekeepers of patient data and, more critically, as frontline caregivers, the health care workforce must be aware of cyber risks and threats. Thus, workers would be more equipped to engage in cybersecurity initiatives (Niki et al., 2022). The lack of employee self-efficacy to protect against ransomware attacks plays a crucial role in the HSE attack. Employees are the first line of defense against cyberattacks and the weakest link in the cyber chain. Organizational culture should incorporate the PMT.

EHR Web Application Attack

A web application is hosted on a remote server and accessed through a client web browser. According to the Verizon data breach report in 2021, healthcare industry web applications were the primary attack vector, with 849 total events analyzed, 571 of which had confirmed data leaks (Alder, 2022). Web application attacks involve attacks on healthcare web applications. The Health Sector Cybersecurity Coordination Center provided a list of web applications commonly used in the healthcare sector, including Electronic Health Record Systems, Patient Portals, Webmail for Hospitals and Clinics, Inventory Management in Hospitals, Health Insurance Portals, Medical Resources for Doctors and Clinical Decision Support, Patient Monitoring Applications with IoT Devices, and Computer-Aided Design Systems for Dentists.

Hackers exploit vulnerabilities in healthcare web applications to gain unauthorized access to EHR/PHI data. This highly sensitive data is lucrative to cybercriminals and individuals interested in using it to submit false billing to obtain federal reimbursement. The top web attacks on healthcare applications include SQL injection attacks, Cross-site scripting, Cross-site Request Forgery, File path traversal, and XML external entity attacks. Improper Asset Disposal, such as disposing of computer hardware and system misconfiguration, could lead to data loss and theft. For instance, due to a system misconfiguration of the Elasticsearch database, 250 million Microsoft customers' records became available online in 2021 (Bischoff, 2020).

Health Industry Cybersecurity Practices (HICP, 2019) stated that hackers frequently obtain lost or stolen mobile devices like laptops, tablets, smartphones, and USB/thumb drives. In 2019, the Office for Civil Rights registered 54 cases of loss or theft, affecting 441,779 people (Office of Human Research Protections, 2024). Data breaches caused by improper asset disposal and system misconfiguration often occur due to human error. Research highlights the limitation of using technological means as the primary solution to cybersecurity issues, identifying the "human factor" as the weakest link in establishing safe and secure digital environments. The PMT could help mitigate the human error associated with cyberattacks and data breaches (Siponen et al., 2023).

Health Industry Cybersecurity Practices

The Health Industry Cybersecurity Practices recommended best practices and security strategies to reduce cybersecurity incidents impacting patient safety. Healthcare organizations should implement security measures such as device encryption, remote wiping capabilities, and mobile device management solutions (MDM) to protect mobile electronics. MDM allows organizations to enforce security policies, monitor device usage, and remotely lock or erase lost or stolen devices. Best practices and cybersecurity strategies include controlling access to sensitive data, creating strong passwords, incident response planning, risk assessment, data encryption, controlling network access, protecting mobile electronics, implementing multifactor authentication, setting up a firewall, keeping software and systems up to date, and using antivirus software.

Email Protection Systems

Email is still a primary target for cyber-attacks, with attackers often using it to carry out data breech activities. Implementing email protection can help mitigate phishing and ransomware attacks and accidental or intentional data loss. Raising awareness through phishing campaigns and security training can remind users of the threats posed by phishing emails. Employees' belief that they could be the target of a phishing attempt affects their perceived threat susceptibility. When the likelihood of an attack is higher, individuals are more likely to be vigilant when reviewing incoming emails and engage in protective behaviors, according to a study by Manoharan et al. (2022).

Using multi-factor authentication whenever possible can add an extra layer of protection against unauthorized access. A recommendation is to avoid communicating sensitive information, such as passwords or credit card details, via email or text message hyperlinks. T. Smit et al. (2021) recommended to be skeptical of emails requesting actions and threatening consequences if the recipient does not comply.

Kessler et al. (2020) found that the Information Security Climate Index (ISCI) is associated with improved employee information security motivation and behavior. The authors suggest using organizational climate literature to influence employee behavior. The study proposes exploring the relationship between the Information Security Climate Index, individuals' motivation toward information security, and their corresponding behaviors. The study also highlights the importance of organizational climate in changing information privacy and security behavior.

NIST 800-50 provides practical security awareness training guidelines and is widely used to train users across multiple industry sectors. The PMT can reinforce the objectives of NIST 800-50. Implementing a robust IT security program requires proper training for IT users, as Wilson and Hash (2003) explained. While email is essential to modern corporate communication, it is also a common target for cyber-criminals using phishing emails. To reduce the risk of cybersecurity compromises and improve cybersecurity posture, a well-structured and thorough phishing training program is essential, as noted by Miranda (2018).

A systematic literature review by Hermanu et al. (2022) evaluated information security in healthcare systems. It highlighted the importance of self-efficacy, perceived severity, and user attitudes or behavior in protecting health information systems. The review also emphasized the role of organizational culture, management action, and managerial support in ensuring information security. Implementing email protection can help mitigate phishing and ransomware attacks and accidental or intentional data loss. Raising awareness through phishing campaigns and security training can remind users of the threats posed by phishing emails. Employees' belief that they could be the target of a phishing attempt affects their perceived threat susceptibility. When the likelihood of an attack is higher, individuals are more likely to be vigilant when reviewing incoming emails and engage in protective behaviors, according to a study by Manoharan et al. (2022).

Relationship Between IT Users and Security Awareness Training

According to NIST 800-50, users are crucial in reducing unintentional errors and vulnerabilities in an organization's IT infrastructure. Users include employees, contractors, visitors, guests, and associates who require access. NIST 800-50 recommends that users should:

- Understand and follow the organization's security policies and procedures.
- Receive adequate training in the rules of behavior for the systems and applications they access.
- Work with management to fulfill training requirements.
- Ensure that software and applications are updated with the latest security patches.
- Be mindful of actions employees can take to protect the organization's information.

These actions include, but are not limited to, using passwords correctly, backing up data, employing proper anti-virus protection, reporting any suspected events or security policy violations, and following procedures to reduce social engineering attacks and the spread of spam, viruses, and worms.

Researcher Contributions

Previous literature has primarily focused on the costs and causes of EHR data breaches, neglecting the strategies to reduce the rising number of breaches. This study addresses this gap by emphasizing the human factor in cyber-attacks and data breaches and proposing strategies to change user behavior and enhance their ability to identify, report, and mitigate threats. The goal is to consider employees and information system users as part of the solution to cyber-attacks rather than a weakness.

EHR records' availability, confidentiality, and integrity are essential for providing quality patient care. Successful cyber-attacks on the healthcare system put patient health at risk, leading to financial and reputational damage for the affected organizations. This research has practical implications for IT security professionals, cybersecurity managers, and CISOs in public and private organizations. The PMT used in this research aligns with the NIST 800-50 (Building Security Awareness Training).

Cyber-attacks and data breaches result from various factors, including human error, employee negligence, malicious attacks, and system users with inadequate knowledge or failure to adhere to security policies. The five data breach types considered in this study are hacking/IT events, inappropriate disposal, unauthorized access, loss, and data theft, all caused by human error. The theoretical framework aims to change user behavior through tailored security awareness training and organizational culture, ultimately reducing cybersecurity incidents in the long term. Changing behavior requires more than just providing knowledge about risks and reactive behaviors. Individuals must understand and apply the advice received exhibit motivation, and be willing to engage in such actions, signifying changes to their attitudes and intentions.

Cybersecurity culture refers to an organization's collective attitudes, actions, knowledge, and awareness of prevalent cyber risks and threats to safeguard information assets. The Energy-Shield project, funded by the European Union to enhance cybersecurity in the electrical power and energy systems, developed the cybersecurity culture framework. The framework offers a technique for assessing security culture indicators in individuals and organizations. The organization's dimensions and areas ensure that it fully addresses its security needs and individuals' specific security concerns. The framework uses various evaluation tools, including surveys and advanced methodologies such as experiments and simulations.

In summary and transition, in Section 3, I shall investigate breaches of EHR data in the U.S. healthcare industry and explore the conceptual framework and scholarly literature, focusing on data breaches in EHRs. The primary cause of data breaches is attributed to human error. This research aims to empower healthcare system users to defend against cyber threats while performing routine tasks. The PMT is recommended for use in healthcare organizations, alongside NIST 800-50, Health Industry Cybersecurity Practices (HICP, 2019), and the Generic Error-Modeling System, to build a robust cyber awareness culture and reduce cybersecurity incidents. Section 3 will delve into the research procedures and methodology, including the research paradigm, design, sampling, data collection, analysis, reliability, and validity.

Section 3: Project Ethics

In this study, I served as the primary data collection instrument by conducting interviews and gathering data from healthcare business managers. Given my professional relationship with the participants, I followed the ethical guidelines outlined in the Belmont Report to safeguard participant rights. I do not supervise any of the interview participants. I used the Belmont Report to protect the rights of participants (Office of Human Research Protections, 2024). Three basic principles from the Belmont Report are particularly relevant to research ethics involving human subjects: respect for persons, beneficence, and justice.

Respect for persons incorporates at least two ethical convictions: first, that individuals should be treated as autonomous agents, and second, that persons with diminished autonomy are entitled to protection. The principle of respect for persons thus divides into two moral requirements: to acknowledge autonomy and protect those with diminished autonomy. An autonomous person can deliberate about personal goals and act in the direction of such deliberation. Respecting autonomy is giving weight to autonomous persons' considered opinions and choices while refraining from obstructing their actions unless they are detrimental to others. To show lack of respect for an autonomous agent is to repudiate that person's considered judgments, to deny an individual the freedom to act on those considered judgments, or to withhold information necessary to make a considered judgment when there are no compelling reasons to do so.

Beneficence is when persons are treated ethically by respecting their decisions, protecting them from harm, and making efforts to secure their well-being. Such treatment falls under the principle of beneficence. The term “beneficence” is often understood to cover acts of kindness or charity beyond strict obligation. In this document, beneficence is understood, in a stronger sense, as an obligation. Two general rules have been formulated as complementary expressions of beneficent actions in this sense: (1) do not harm and (2) maximize possible benefits and minimize possible harms.

Informed consent is respect for persons that requires subjects, to the degree that they are capable, be allowed to choose what shall or shall not happen to them. This opportunity is provided when adequate standards for informed consent are satisfied. While the importance of informed consent is unquestioned, controversy prevails over the nature and possibility of informed consent. Nonetheless, there is widespread agreement that the consent process can be analyzed as containing three elements: information, comprehension, and voluntariness.

In the informed consent form, I invited participants to take part in an interview about their professional experiences. I expanded upon the interview procedures, describing the purpose of my study for my Doctorate of Business Administration research, research questions, and interview questions. I described the voluntary nature of the study, the risks and benefits of being in the study, and the privacy procedures for the interview recordings and transcripts recordkeeping process for a minimum of 5 years with all confidential data removed. A phone number was provided to participants to discuss their rights as participants, including the decision to withdraw from the study. I spelled out that my participants would not be incentivized to participate in this study.

I used alpha-numeric symbols to represent the participants (e.g., P1, P2, P3, etc.) to protect the confidentiality of their names. I organized all data files so that the participants' identity remains confidential. Interview recordings and transcripts will be stored in a locked safe for at least 5 years. At the end of the 5 years, the data will be removed and destroyed to protect the confidentiality of participants. Adhering to Walden University Institutional Review Board guidelines to protect participant privacy, I obtained approval from the Institutional Review Board (Walden University ethics approval number (11-05-24-1181522) before commencing data collection**.**

Nature of the Project

Of the three research methodologies are qualitative, quantitative, and mixed (Saunders et al., 2019), I chose the qualitative research approach for my project. It is appropriate because it provides in-depth insight into individuals' experiences, thoughts, and feelings (Yadav, 2022). Qualitative data can aid in understanding the factors that affect the actions and choices of individuals. A qualitative and mixed method study is not appropriate, as the research does not use quantifiable data but rather *rich data and thick descriptions*. The qualitative method was considered the most suitable for my study, which aimed to investigate a research problem without comparing variables using numerical data or conducting hypothesis testing.

Kelly and Cordeiro (2020) indicated that a qualitative research method with a pragmatic inquiry as the specific research design addresses the research question in most qualitative studies. The pragmatic inquiry design also offers a balance of participant perspectives, increases efficiency, broadens the scope of the research, and promotes high-quality study results (Ramanadhan et al., 2021). Researchers often use pragmatic inquiry design to study organizational processes (Kelly & Cordeiro, 2020). One of the principles of pragmatic inquiry is that research produces practical, action-oriented results designed to solve a business problem (Kelly & Cordeiro, 2020). The design was appropriate for the goals of this study, which was to identify and explore effective strategies healthcare business managers use to reduce data breaches successfully.

Population, Sampling, and Participants

The population for this study consisted of six healthcare business managers who have successfully used strategies to reduce data breaches. The eligibility criteria for the study participants is, 1) Currently employed as health care business managers, 2) has worked at a major university hospital for over 2 years, and 3) has successful strategies to reduce data breaches.

I identified and accessed participants through professional networking using social media. I communicated with the identified participants through phone calls, emails, and social media to gain access and develop a working relationship. I explained the study's purpose, process, and data collection process to the participants. I also explained to study participants that participation is voluntary, the process to implement informed consent, and clarify that they might withdraw from the study at any time. The study participant characteristics are aligned with the overarching project purpose of identifying strategies that can be used to reduce data breaches in a healthcare setting. I used purposive sampling to choose participants to improve the reliability of the study. According to Campbell et al. (2020), characteristics of purposeful sampling include dependability, transferability, credibility, and confirmability.

Data Collection Activities

Once I received approval from the Institutional Review Board (IRB), I emailed potential participants an invitation to participate. It contained a summary of the research project (see Appendix B). After the participants accepted the invitation and provided a signed consent, I scheduled them for an interview with me. At the start of the interview process, I clarified the project's objectives and reaffirm the participants' right to withdraw from the study at any time. All interviews were conducted via video calls or phone interviews using semistructered interviews and audiorecorded with the participants' consent. I followed an interview protocol to ensure I asked the same questions in the same order and provide the same information to each participant to prevent bias and ensure consistency. This process also supports ensuring reliability (Tourangeau, 2020). During and after each interview, I documented my reflections and participant feedback on the interview process or questions. At the end of each interview, I set a date and time to conduct member checking with the participant to validate the accuracy of my interpretations of their responses. Member checking aided in ensuring the accuracy of the data collected (McKim, 2023).

Member Checking

To ensure validity in qualitative research, it is crucial to conduct member checking (Caretta & Pérez, 2019). McKim (2023) highlighted the significance of validity in qualitative studies and emphasized the need for credibility in research. To improve the credibility of my research, I provided each participant with a summary of my interpretations of their statements for their review. Participants were provided sufficient time to review their interview summaries and notify me of their acceptance or of any inaccuracies. Member checking strengthens researcher-participant relationships and verifies that the data accurately reflects participants' experiences and perspectives, consequently maximizing the study's validity (McKim, 2023).

Interview Questions

1. What successful strategies have you implemented to reduce data breaches?
2. How did you measure the success of the strategy?
3. What challenges did you encounter when implementing the strategies to reduce data breaches?
4. How did you over come the challenges?
5. What was the impact of the implemented strategy on profitability?
6. How would you describe the personal threat rating of the data breaches after implementing your successful strategies?
7. What other information regarding your successful strategies to reduce data breaches and sustain profitability that we have not already been discussed would you like to share?

Data Organization and Analysis Techniques

I used journal entries, research logs, and cataloging and labeling system techniques during the interview to ensure data organization and my understanding of the data collected. For the interview process, I used a digital recording device and take written notes. I used the software Microsoft Excel and Microsoft Word to identify themes within the data. I labeled the participants P1, P2, P3, etcetera to protect the identity of the interviewees and the companies for which they work. I stored all information onto a protected thumb drive, and it will be destroyed after 5 years.

Throughout my data analysis process, I conducted both thematic and narrative analyses to examine the collected data. According to Naeem et al. (2023), thematic analysis involves exploring patterns of meaning in a data set by making it a flexible and widely used approach that aligns well with various qualitative research designs. Braun et al. (2022) stated this process includes identifying, analyzing, and reporting patterns (themes) within qualitative data sources such as interviews, observations, and documents. I organized all documents, interview transcripts, and audio recordings in a directory with pseudonyms for each participant. Using thematic analysis, I examined the qualitative data to identify recurring themes and patterns, providing insights by examining data breach prevention strategies using the PMT conceptual framework. I conducted interviews using Microsoft Teams and transcribed the audio using Microsoft Word. Next, I transcribed all the materials and completed a member-check; I saved all the data and audio files on a password-protected flash drive. Once my research was complete, I deleted the data and will keep the flash drive in a safe and locked location for a period of 5 years.

Reliability and Validity

Reliability

Reliability is a critical aspect of all research studies. Adler (2022) explained qualitative research; reliability refers to the robustness of the research methodology, design, sampling method, and data analysis. Rose and Johnson (2020) described that researchers can enhance the reliability of qualitative research by employing various strategies such as (a) acknowledging and disclosing any researcher biases or preconceived assumptions, (b) rigorously outlining the methods for participant recruitment, data collection, and analysis, and (c) accurately reporting the information provided by the participants. Following these guidelines, I implemented multiple measures, including thorough researcher reflexivity protocols, to strengthen the reliability and dependability of the study.

Dependability

Rose and Johnson (2020) specified that dependability is a critical approach for researchers to establish the rigor and trustworthiness of qualitative studies that rely on rigorous data collection and analysis protocols. In this study, I emphasized the dependability of my findings through three main strategies. Firstly, I meticulously documented my research protocols in a dedicated research log to ensure the rigorous establishment of participants and research methods. According to Johnson et al. (2020), maintaining a research log enhances methodological rigor by enabling researchers to document their methodological choices comprehensively. Secondly, I maintained a reflexivity journal to record my initial notions and reflections at each stage of the research process. A reflexive journal enables researchers to recognize potential biases (Peddle, 2021). Lastly, I utilized member checking to allow participants to validate my interpretation of their data. Research by Caretta and Perez (2019) found member checking to be a vital mechanism qualitative researchers employ to bolster the trustworthiness of their study findings. These methodological approaches reinforced the dependability of the study's findings.

Validity

Validity is another crucial aspect of research studies. One method in which qualitative researchers can improve the validity of their findings is through data triangulation and data saturation (Moon, 2019). Qualitative researchers achieve external validity, or transferability, in multiple case studies by evaluating multiple cases, using triangulation, and, most importantly, by comparing their findings to those in the academic literature (Stahl & King, 2020). This comparison validates the research approach and enhances the credibility of the study. The validity of a qualitative study is assessed through credibility, transferability, confirmability, and trustworthiness. This section of the study will conclude with a discussion of these elements, as well as data saturation.

Credibility

Credibility refers to the confidence of the data collected in qualitative research. Rose and Johnson (2020) illustrated that researchers can use robust designs to strengthen their studies' credibility and ensure that the collected data adequately addresses the research topic. In qualitative research, member checking is one of the most crucial techniques for establishing credibility. Caretta and Perez (2019) defined member checking as the recommended procedure of providing the participants with a copy of the researcher's interpretation of the study's findings for review and confirmation. Member checks can be a crucial component for establishing credibility or authenticity; however, according to Candela (2019), there are typical problems with member checks, including a lack of response from most participants, creating additional intrusion for participants, little or no substantive changes in research findings, and the need for additional project resources. Moon (2019) conferred that researchers using the qualitative methodology must use various sources and triangulate them to increase credibility. According to Valencia (2022), methodological triangulation involves using multiple data collection methods. I collected data from business websites, financial reports, observation notes, and face-to-face interviews. I used triangulation to enhance the credibility of my qualitative research. To ensure the findings are credible, I implemented the following steps: (a) select and verify participants, (b) member checking, (c) triangulation, and (d) usage of field-based data collected, such as journals, writings, and artifacts. Collectively, the additive or comprehensive uses of these tools and instruments can foster increased rigor and transparency around the research, increasing confidence, trustworthiness, and credibility surrounding research design, data collection, data analysis, findings, and qualitative interpretations (Johnson et al., 2020). The sample size of my study, member checking, and the steps I have outlined created a strong sense of credibility of my study's results.

Transferability

Transferability is like the concept of generalizability in quantitative studies. Specifically, transferability refers to the ability to apply the research findings to other cases with similar individuals (Rose & Johnson, 2020). Johnson et al. (2020) indicated that thoroughly documenting methodological choices can promote the transferability of a study's findings. To address transferability, I rigorously documented my data collection and analysis methods and provid a detailed description of the interview protocol, case study, participants, and research findings. According to Campbell et al. (2020), the purposeful sampling technique can also enhance the transferability of a study's findings by allowing diverse participants to be selected. I addressed transferability by ensuring that the purposefully selected participants interviewed in the study are diverse and representative of the study's general population. I also addressed transferability by making certain that I spelled out the steps I intend to follow so my work can be replicated by other researchers.

Confirmability

Confirmability refers to the extent to which other researchers can replicate the findings. A recent study by Strijker (2020) found the confirmability of a study can be enhanced by rigorously documenting the study's anticipated and actual methodology. According to Adeoye-Olatunde and Olenik (2021), the use of an interview protocol can enhance confirmability by ensuring that researchers ask all participants questions in the same order. To confirm my study's accuracy, I used an interview protocol to conduct the semistructured interviews. Prosek and Gibson (2021) concluded that ensuring the accuracy of interview transcripts is another mechanism for promoting confirmability. Therefore, I accurately documented the interview transcripts and compare them line-by-line with the interview audio recordings. Stahl and King (2020) concluded that confirmability can also be promoted through researcher reflexivity. To minimize researcher bias, I used reflexivity protocols, including journaling, to document my perceptions as the researcher.

Data Saturation

Data saturation is important for confirmability and trustworthiness. Data saturation is when no new information will be gained by interviewing more participants (Guest et al., 2020). Once saturation has been reached, data collection is thought to be exhausted (Guest et al., 2020). I interviewed six health care business managers who met my inclusion criteria. I reached data saturation with six participants, however if I did not then I would have continued to interview participants until such time as I did achieve data saturation.

Transition and Summary

In Section 3, I detailed the methodology for the research project, which aims to identify strategies health care business managers use to reduce data breaches. The discussion included an examination of ethical considerations in research and a detailed description of the project's scope. I provided insights into the target population, sampling methods, and participant selection process to ensure the relevance of the collected information to the research objectives. Details on data collection procedures, organization, and analysis techniques, including the utilization of ATLAS.ti software, were also covered. I highlighted the practice of member checking to validate research findings. Additionally, I created a set of interview questions focused on obtaining information regarding successful strategies used by healthcare business managers to reduce data breaches. Finally, I emphasized the significance of ensuring the research's reliability, validity, and overall goal of obtaining and reaching data saturation.

Section 4: Findings and Conclusions

Presentation of the Findings

The purpose of this qualitative pragmatic inquiry was to identify and explore the effective strategies some health care business managers use to reduce data breahes and sustain profitability. I conducted semistructured interviews with six business leaders who have experience implementing data breach strategies for 24 months or more. I also utilized publicly available documents, including successful data breach prevention strategies, to support my data analysis in determining the effective approaches healthcare business managers use to minimize data breaches and reduce impact on profitability.

I conducted the one-on-one interviews via Microsoft Teams and recorded the audio for transcription. Data validation was conducted through member checking while the data coding was done using Microsoft Word and Excel software, following Braun's thematic analysis framework (Braun et al., 2022). The analysis uncovered four themes of strategies healthcare business managers use to reduce data breaches including (a) identifying vulnerabilities through threat appraisal (b) improving response efficacy through coping appraisal (c) effort through response cost, and (d) building protection motivation through intent to act. The themes are listed in the following table.

Table 2

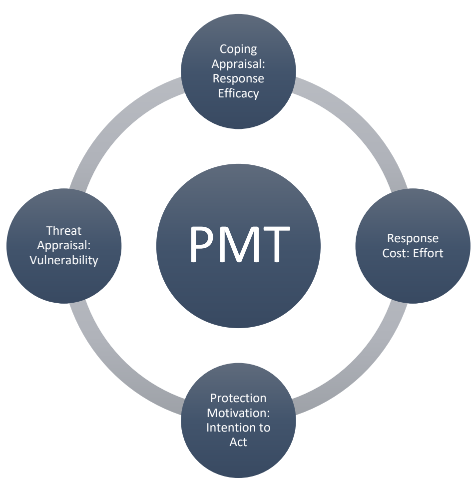
References of Major Themes

Major theme	Participants	References
Theme 1: Coping appraisal-Response efficacy	6	48
Theme 2: Response cost- Effort	5	14
Theme 3: Threat appraisal-Vulnerabilities	6	20
Theme 4: Protection motivation-Intent to act	4	8

The themes aligned to the PMT, which was the conceptual framework for this project. According to Rogers (1975), organizations are motivated to take protective measures when the perception of significant threat is high and hold the belief to mitigate threats successfully. Data breaches in the United States are the costliest and the most frequent in the world (IBM, 2023). Therefore, it is recommended in business environments to implement proven successful strategies to reduce data breaches while maintaining profitability. The above themes reflect strategies that strengthen internal capabilities in light of growing cybersecurity threats.

Figure 4

A Summary of the Themes



Theme 1: Coping Appraisal - Response Efficacy

One of the emerging themes from the responses of participants was the response efficacy of coping mechanisms in reducing data breaches. The participants indicated that measures to prevent data breaches included using two-factor authentication, VPN usage, and phishing tests. Offensive measures serve a significant role in increasing health data security. For instance, P1 underlined that frequent phishing email tests were necessary for making employees more vigilant regarding potential hazards. Also, P2 mentioned moving files to secure cloud platforms, such as OneDrive, which provide them with greater facilities of tracking and restricted access, hence securing sensitive information. Such findings support the studies by Xiao et al. (2021) that clearly showed that a multi-dimensional approach to coping mechanisms was highly relevant for effectively mitigating risks.

Overall, participants recognized that implementation of such strategies at an organizational level provides solid security frameworks. P3 mentioned that phishing detection systems and employee training helped develop a culture of security awareness. These observations align with Bayl-Smith et al. (2021) findings that similar strategies increase organizational resilence. Besides securing the data, such measures ensure that various stakeholders have confidence that the organization seriously handles data protection.

Theme 2: Response Cost - Effort

Another recurring theme was the cost and effort involved in implementing data protection strategies. Testimonies shared the difficulty in the early adoption stages, with a significant concern on employee resistance to change. For example, P6 spoke of the

Luddite attitude from employees who did not want to use multi-factor authentication since this was too inconvenient and required additional steps. These challenges notwithstanding, participants indicated that persistence in training and a clear explanation of the reasons underlying these measures helped to break the resistance. P2 stressed setting clear deadlines and constant reminders to encourage compliance. This finding aligns with Lemay et al. (2020), who stressed the need for clear communication and training to counteract employee reluctance. Although resource-intensive, this work is consistent with the findings of Andronache (2021), whose study highlights the role of leadership in effective organizational culture change. Sulaimen et al. (2022) indicated that even though the response costs may be high initially, reduced vulnerability justifies investment in the long term.

Theme 3: Threat Appraisal Vulnerability

Another leading theme identified by the participants was the importance of vulnerability assessment in comprehending possible threats. P1 identified that recent breaches in peer organizations served as a grim reminder of the consequences of poor security measures. This proactive thinking led the organization to invest in state-of-the-art security tools, including shared drives that allow access on a need-to-know basis with multi-layered authentications. These findings aling with Rogers (1975), who emphasized that the perception of vulnerability is a key motivator for protective behavior in PMT.

P5 highlighted that patients' sensitive information had to be protected at all costs since a breach would have adverse implications in terms of financial and reputational losses. This is further supported by Sulaiman et al. (2022), who identified that the awareness of vulnerabilities and consequences strengthens organizational commitement to security measures. Kapoor et al. (2021) noted that awareness of these vulnerabilities provides healthcare organizations a clearer understanding of the most critical risks.

Theme 4: Protection Motivation - Intention to Act

The last theme was the intention to act as a protective mechanism. The respondents discussed how protection measures became institutionalized within the organization's culture. For example, P1 said that using VPNs and other security tools has become second nature to the employees; thus, it is an attitudinal change fostered by organizational policy and practice. Furthermore, respondents pointed out continuous education and the ability to adapt to constantly changing threats. This aligns with the Bayl-Smith et al. (2021) finding that cultivating a proactive security mentality is fundatmental in embedding organizational resilience. P6 explained that other ways of maintaining high-security awareness involve setting up a proactive attitude among workers. These results align with Rogers (1975), who highlighted the importances of organizations to lead protective behaviors using PMT.

Business Contributions and Recommendations for Professional Practice

This project is significant as the results provide actionable insights in the light of PMT for health and business leaders who aim to promote data security. These findings identify the critical roles of reducing data breaches through multi-factor authentication, VPNs, phishing training, and cloud storage. These measures, therefore, address the balance between technological adoption and behavioral change on critical themes such as Coping Appraisal or Response Efficacy, Response Cost or Effort, Threat Appraisal or Vulnerability, and Protection Motivation or Intention to Act. These findings align with

Sulaiman et al. (2022), who correlated the imporance of integrating protective strategies to reduce and prevent cyber security risks.The applied practical conceptual findings reduce human resistance to new processes through effective communication and training, building a proactive security compliance and preparedness culture.

Healthcare business leaders should first familiarize themselves with the cybersecurity framework, smoothen the flow of processes to reduce the effort employees put in, and create a watchful culture. Further regular risk assessments and investment in innovative technologies, including AI and IoT, help to add greater resilience to data breaches. Automated processes help bridge gaps in existing understanding through practical applications for improving business outcomes while securing sensitive data. These insights align with Kapoor et al. (2021), who discovered the value of innovative technologies in maintaining organizational defenses against emerging threats. The dissemination could be done through journals, conferences within the industry, and in-house training programs to reach the relevant stakeholders and bring effective improvement in business practices for enhanced profitability.

Implications for Social Change

This work provides significant implications for positive social change, in particular for data security in healthcare organizations. Using PMT, the study points out concrete ways through which organizational resilience is not only enhanced but the dignity and privacy of individuals whose sensitive information is at risk. Adopting various security technologies, such as multi-factor authentication, phishing awareness training, and secure cloud systems by these organizations, demonstrates the essential commitment to patient data protection in the trust between health providers and their communities.

These findings foster a culture of proactive cybersecurity at the broader social level. This culture reduces the possibility of data breaches, one nightmare that has devastated many individuals and communities. It ensures that the healthcare system remains resilient, with continuous service access by all and reduced economic and psychological burdens in case of breaches. Recommendations from this study put organizations at the front line, serving as stewards of societal trust, a protection core to an individual's worth and dignity, through addressing vulnerabilities and creating a culture of vigilance. When delivered through education, training, and policy development, such findings may catalyze systemic improvement by bettering institutional and societal practices for robust data management and cybersecurity.

Recommendations for Further Research

Future research projects are needed to overcome the limitations identified and build upon the findings of this study by expanding their scope outside health into other industries, such as finance, education, and retail, to explore cybersecurity strategies in several industries. Studies broader in scope could also improve the generalizability of these results and reveal broader best practices for reducing data breaches. However, small and medium-sized organizations, especially those not part of a major hospital network, may provide insights into how size, resources, and organizational structures modify the effectiveness of mitigation strategies for data breaches and offer scalable solutions adaptable to different organizational contexts. The study may add participants from different departments to determine variances in size and culture in cybersecurity defenses.

Longitudinal studies allow for observing how cybersecurity strategies evolve, accounting for disparities in participant experience and organizational familiarity. Longitudinal studies on effective training programs and communication strategies follow organizations that enable employees to fully engage in cybersecurity practices to address new managers' peculiar challenges in adopting past efforts. Future studies should also explore the influence of organizational culture, including leadership styles and training policies, on the successful implementation of cybersecurity measures. A mixed-methods approach to validation, such as surveys and statistical analyses, is recommended to help triangulate the qualitative findings with measurable data. Finally, the study could investigate how organizations adapt to evolving external threats such as ransomware and phishing schemes and, in so doing, develop global insights into trends and innovative solutions. These will address the grey areas, add to the study's limitations, and consolidate a better understanding of practical strategies to improve business practices and reduce data breaches. Application of the study’s findings will support Rogers (1975), who emphasized the role of protective behaviors in fostering the common social good.

Conclusion

Any business leader faces challenges in identifying effective strategies to reduce data breaches while maintaining operational efficiency and profitability. Without comprehensive measures, these challenges can result in significant financial losses and reputational harm. This qualitative study focused on identifying the successful cybersecurity strategies employed by healthcare business managers to mitigate data breaches. The findings offer actionable insights into how organizations can strengthen their data security frameworks by leveraging technological solutions and cultural shifts.

Using PMT as the study's conceptual framework, this project identified four key themes: coping appraisal (response efficacy), response cost (effort), threat appraisal (vulnerability), and protection motivation (intention to act). These themes encapsulate a systematic approach to addressing cybersecurity threats. The insights provided by this research have the potential to help business leaders implement robust data security strategies, protect sensitive information, and foster organizational resilience. Organizations can significantly reduce risks, enhance stakeholder trust, and improve business continuity and profitability by adopting these measures.

References

Adeoye-Olatunde, O. A., & Olenik, N. L. (2021). Research and scholarly methods: Semi-structured interviews. *Journal of the American College of Clinical Pharmacy*, *4*(10), 1358–1367. https://doi.org/10.1002/jac5.1441

Adler, R. (2022). Trustworthiness in qualitative research. *Journal of Human Lactation*. *38*(4), 598–602. https://doi.org/10.1177/08903344221116620

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. Sciencedirect. https://doi.org/10.1016/0749-5978(91)90020-T

Alder, S. (2022). Verizon data breach investigations report reveals 2021 data breach trends. *HIPAA Journal*. https://www.hipaajournal.com/verizon-data-breach-investigations-report-reveals-2021-data-breach-trends/

Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences*, *11*(8), 3383. https://doi.org/10.3390/app11083383

Alohali, M., Clarke, N., Li, F., & Furnell, S. (2018). Identifying and predicting the factors affecting end-user's risk-taking behavior. *Information and Computer Security, 26*(3), 306–326. https://doi.org/10.1108/ICS-03-2018-0037

Andronache, A. (2021). Increasing security awareness through lenses of cybersecurity culture. *Journal of Information Systems & Operations Management, 15*(1), 7–22. https://www.proquest.com/scholarly- journals/increasing-security-awareness-through-lenses/docview/2571982600/se-2

APWG. (2022a). Phishing activity trends report Q4 2021. In *APWG* (pp. 1–15). https://docs.apwg.org/reports/apwg_trends_report_q4_2021.pdf?_gl=1

APWG. (2022b). Phishing activity trends report Q3 2022 In *APWG* (pp. 1–10). https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf?_gl=1*od5kx0*_ga*MTY3NjYwNzYzNy4xNzIzMDU0OTk4*_ga_55RF0RHXSR*MTcyMzA1NDk5Ny4xLjEuMTcyMzA1NTQ1MS4wLjAuMA

Bayl-Smith, P., Taib, R., Yu, K., & Wiggins, M. (2021). Response to a phishing attack: Persuasion and protection motivation in an organizational context. *Information & Computer Security, 30*(1), 63–78. https://doi.org/10.1108/ics-02-2021-0021

Bischoff, P. (2020). 250 million Microsoft customer service & support records exposed. *Comparitech*. https://www.comparitech.com/blog/information-security/microsoft-customer-service-data-leak/

Braun, V., Clarke, V., & Hayfield, N. (2022). 'A starting point for your journey, not a map': Nikki Hayfield in conversation with Virginia Braun and Victoria Clarke about thematic analysis. *Qualitative Research in Psychology*, *19*(2), 424–445. https://doi.org/10.1080/14780887.2019.1670765

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). Purposive sampling: Complex or simple? Research case examples. *Journal of Research in Nursing*: JRN, *25*(8), 652–661. https://doi.org/10.1177/1744987120927206

Caretta, M., & Pérez, M. (2019). When participants do not agree: Member checking and challenges to epistemic authority in participatory research. *Field Methods, 31*(4), 359–374. https://doi.org/10.1177/1525822X19866578

Daniel, B., & Wald, N. (2019). Demystifying the meaning and role of conceptual and theoretical frameworks in postgraduate research education. *Proceedings of the 18th European Conference on Research Methodology for Business and Management Studies*. https://doi.org/10.34190/rm.19.123

DeJonckheere, M., & Vaughn, L. (2019). Semistructured interviewing in primary care research: A balance of relationship and rigour. *Family Medicine and Community Health, 7*(2). https://doi.org/10.1136/fmch-2018-000057

Desouza, K. C., Ahmad, A., Naseer, H., & Sharma, M. (2020). Weaponizing information systems for political disruption: The Actor, Lever, Effects, and Response Taxonomy (ALERT). *Computers & Security*, *88*, 101606. https://doi.org/10.1016/j.cose.2019.101606

Durkin, J., Jackson, D., & Usher, K. (2020). Qualitative research interviewing: Reflections on power, silence and assumptions. *Nurse Researcher*, *28*(4), 31–35. https://doi.org/10.7748/nr.2020.e1725

Fox, B., & Holt, T. J. (2020). Use of a multitheoretic model to understand and classify juvenile computer hacking behavior. *Criminal Justice and Behavior*, 009385482096975. https://doi.org/10.1177/0093854820969754

Guest, G., Namey, E., & Chen, M. (2020). A simple method to assess and report thematic saturation in qualitative research. *PLoS One*, *15*(5), 1–17. https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0232076

Hathaliya, J. J., & Tanwar, S. (2020). An exhaustive survey on security and privacy issues in Healthcare 4.0. *Computer Communications*, *153*(1), 311–335. https://doi.org/10.1016/j.comcom.2020.02.018

Hermanu, A. I., Sondari, M. C., Dimyati, M., & Sari, D. (2022). Study on university research performance based on systems theory: Systematic literature review. *International Journal of Productivity and Quality Management*, *35*(4), 447. https://doi.org/10.1504/ijpqm.2022.122777

HICP. (2019). Exploring the health industry cybersecurity practices (HICP) publication, How to use it. Healthtech Security; *TechTarget.* https://www.techtarget.com/healthtechsecurity/feature/Exploring-the-Health-Industry-Cybersecurity-Practices-HICP-Publication-How-to-Use-It

Hull, G., John, H., & Arief, B. (2019). Ransomware deployment methods and analysis: views from a predictive model and human responses. *Crime Science, 8*(1). https://doi.org/10.1186/s40163-019-0097-9

IBM. (2023). *Cost of a data breach 2023*. IBM. https://www.ibm.com/reports/data-breach

Jalali, M. S., Bruckes, M., Westmattelmann, D., & Schewe, G. (2020). Why employees (still) click on phishing links: Investigation in hospitals. *Journal of Medical Internet Research, 22*(1)https://doi.org/10.2196/16775

Johnson, J., Adkins, D., & Chauvin, S. (2020). A review of the quality indicators of rigor in qualitative research. *American Journal of Pharmaceutical Education*, *84*(1), 138–146. https://doi.org/10.5688/ajpe7120

Kam, H. J., Mattson, T., & Kim, D. J. (2020). The "right" recipes for security culture: a competing values model perspective. *Information Technology & People, 34*(5), 1490–1512. https://doi.org/10.1108/itp-08-2019-0438

Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2021). Ransomware detection, avoidance, and mitigation scheme: A review and future directions. *Sustainability*, *14*(1), 8. https://doi.org/10.3390/su14010008

Karambelas, C. (2020). Health care technology: Ransomware risk and protection. *American Bankruptcy Institute Journal, 39*(5), 30-31,56-57. https://www.proquest.com/scholarly-journals/health-care-technology-ransomware-risk-protection/docview/2407574230/se-2

Kelly, L., & Cordeiro, M. (2020). Three principles of pragmatism for research on organizational processes. *Methodological Innovations*, *13*(2). https://doi.org/10.1177/2059799120937242

Kessler, S. R., Pindek, S., Kleinman, G., Andel, S. A., & Spector, P. E. (2020). Information security climate and the assessment of information security risk among healthcare employees. *Health Informatics Journal, 26*(1), 461-473. https://pubmed.ncbi.nlm.nih.gov/30866704/

Kuppusamy, P., Samy, G. N., Maarop, N., Magalingam, P., Kamaruddin, N., Shanmugam, B., & Perumal, S. (2020). Systematic literature review of information security compliance behaviour theories. *Journal of Physics:*

Conference Series, *1551*, 012005. https://doi.org/10.1088/1742-6596/1551/1/012005

Lemay, D., Basnet, R., & Doleck, T. (2020). Examining the relationship between threat and coping appraisal in phishing detection among college students. *Journal of Internet Services and Information Security (JISIS)*, 10(1) 38-49. https://doi.org/10.22667/JISIS.2020.02.29.038

Li, W., Liu, R., Sun, L., Guo, Z., & Gao, J. (2022). An investigation of employees' intention to comply with information security system—A mixed approach based on regression analysis and fsQCA. *International Journal of Environmental Research and Public Health*, *19*(23), 16038. https://doi.org/10.3390/ijerph192316038

Manoharan, S., Katuk, N., Hassan, S., & Ahmad, R. (2022). To click or not to click the link: The factors influencing internet banking users' intention in responding to phishing emails. *Information & Computer Security*, ahead-of-print(ahead-of-print). https://doi.org/10.1108/ics-04-2021-0046

Marikyan, D., & Papagiannidis, S. (2023). Protection motivation theory: A review. *TheoryHub Book: This handbook is Based On The Online Theory Resource: TheoryHub*, 78-93. https://open.ncl.ac.uk/theory-library/TheoryHubBook.pdf

McKim, C. (2023). Meaningful member-checking: A structured approach to member-checking. *American Journal of Qualitative Research*, *7*(2), 41–52. https://www.ajqr.org/article/meaningful-member-checking-a-structured-approach-to-member-checking-12973

Miranda, M. (2018). Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach. *International Management Review*, *14*(2). http://americanscholarspress.us/journals/IMR/pdf/IMR-2-2018/IMR-v14n2art1.pdf

Moon, M. D. (2019). Triangulation: A method to increase validity, reliability, and legitimation in clinical research. *Journal of Emergency Nursing*, *45*(1), 103–105. https://doi.org/10.1016/j.jen.2018.11.004

Mou, J., Cohen, J., Bhattacherjee, A., & Kim, J. (2022). A test of protection motivation theory in the information security literature: A meta-analytic structural equation modeling approach in search advertising. *Journal of the Association for Information Systems*, *23*(1), 196–236. https://doi.org/10.17705/1jais.00723

Moustafa, A. A., Bello, A., & Maurushat, A. (2021, June 18). The role of user behaviour in improving cyber security management. *Frontiers in psychology*, 12(561011), 1-9. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8253569/

Naeem, M., Ozuem, W., Howell, K., & Ranfagni, S. (2023). A step-by-step process of thematic analysis to develop a conceptual model in qualitative research. *International Journal of Qualitative Methods*, *22*, Article e16094069231205789. https://doi.org/10.1177/16094069231205789

Niki, O., Saira, G., Arvind, S., & Mike, D. (2022). Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that. *Digital Health*, *8*, 205520762211046. https://doi.org/10.1177/20552076221104665

Office for Human Research Protections. (2024). *The Belmont Report*. U.S. Department of Health and Human Services; U.S. Department of Health and Human Services. https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html

Peddle, M. (2021). Maintaining reflexivity in qualitative nursing research. *Nursing Open*, *9*(6). https://doi.org/10.1002/nop2.999

Ponemon Institute. (2023). Cybersecurity in healthcare: The cost and impact on patient safety and care. Proofpoint.com 1-58. https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf

Prosek, E. A., & Gibson, D. M. (2021). Promoting rigorous research by examining lived experiences: A review of four qualitative traditions. *Journal of Counseling & Development*, *99*(2), 167–177. https://doi.org/10.1002/jcad.12364

Ramanadhan, S., Revette, A., & Lee, R. (2021). Pragmatic approaches to analyzing qualitative data for implementation science: An introduction. *Implementation Science Community 2*(1). https://doi.org/10.1186/s43058-021-00174-1

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

Rose, J., & Johnson, C. (2020). Contextualizing reliability and validity in qualitative research: Toward more rigorous and trustworthy qualitative social science in leisure research. *Journal of Leisure Research*, *51*(4), 432-451. https://doi.org/10.1080/00222216.2020.1722042

Ross, P., & Bibler Zaidi, N. (2019). Limited by our limitations. *Perspectives on Medical Education*, *8*(4), 261–264. https://doi.org/10.1007/s40037-019-00530-x

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2019). *Research Methods for Business Students*. 8th Edition, Pearson, New York.

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare data breaches: Insights and implications. *Healthcare*, *8*(2), 133. NCBI. https://doi.org/10.3390/healthcare8020133

Shahbaznezhad, H., Rashidirad, M., & Vaghefi, I. (2019). A systematic review of the antecedents of knowledge transfer: an actant-object view. *European Business Review*, *31*(6), 970–995. https://doi.org/10.1108/ebr-07-2018-0133

Siponen, M., Rönkkö, M., Fufan, L., Haag, S., & Laatikainen, G. (2023). Protection motivation theory in information security behavior research: reconsidering the fundamentals. *Communications of the Association for Information Systems*, *53*(1), 47. https://aisel.aisnet.org/cais/vol53/iss1/47/

Smit, T., van Haastrecht, M., & Spruit, M. (2021). The effect of countermeasure readability on security intentions. *Journal of Cybersecurity and Privacy*, *1*(4), 675–704. https://doi.org/10.3390/jcp1040034

Stahl, N. A., & King, J. A. (2020). Expanding approaches for research: Understanding and using trustworthiness in qualitative research. *Journal of Developmental Education, 44*(1), 26-28. https://files.eric.ed.gov/fulltext/EJ1320570.pdf

Strijker, D. B. (2020). Research methods in rural studies: Qualitative, quantitative and mixed methods. *Journal of Rural Studies, 78*, 262-270. https://doi.org/10.1016/j.jrurstud.2020.06.007

Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity behavior among government employees: The role of protection motivation theory and responsibility in mitigating cyberattacks. *Information*, *13*(9), 413. https://doi.org/10.3390/info13090413

Tourangeau, R. (2020). Survey reliability: Models, methods, and findings. *Journal of Survey Statistics and Methodology*, *9*(5). https://doi.org/10.1093/jssam/smaa021

Valencia, M. M. A. (2022). Principles, scope, and limitations of the methodological triangulation. *Investigacion Y Educacion En Enfermeria*, *40*(2), 1–14. https://doi.org/10.17533/udea.iee.v40n2e03

Van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies*, *123*, 29–39. https://doi.org/10.1016/j.ijhcs.2018.11.003

Walden University. (2024). *SkillsFirst Interview Questions Guide*. https://academicguides.waldenu.edu/ld.php?content_id=69325561

Wang, Z., Sun, L., & Zhu, H. (2020). Defining social engineering in cybersecurity. *IEEE Access, 8*, 85094-85115. https://doi.org/10.1109/access.2020.2992807

Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. *NIST Special Publication*, 800(50), 1-39. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

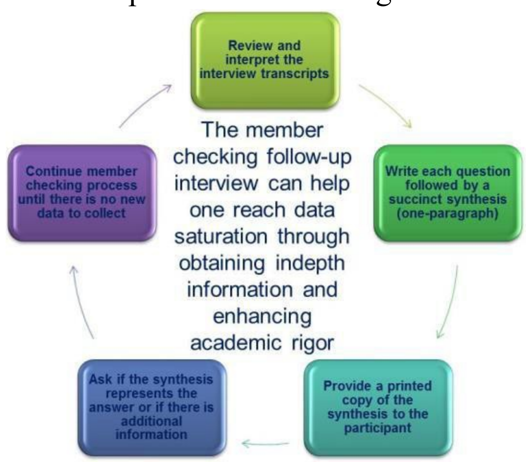
Xiao, Q., Liu, X., Wang, R., Mao, Y., Chen, H., Li, X., Liu, X., Dai, J., Gao, J., Fu, H., & Zheng, P. (2021). Predictors of willingness to receive the COVID-19 vaccine after emergency use authorization: The role of coping appraisal. *Vaccines*, *9*(9), 967. https://doi.org/10.3390/vaccines9090967

Yadav, D. (2022). Criteria for good qualitative research: A comprehensive review. Asia-Pacific Education *Research*, *31(6),* 679–689. https://doi.org/10.1007/s40299-021-00619-0

Yeo, L. H., & Banfield, J. (2022). Human factors in electronic health records cybersecurity breach: An exploratory analysis. *Perspectives in Health Information Management*, *19*(Spring). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9123525/

Appendix A: Interview Protocol

Interview Protocol	
Introduce the interview and set the stage. Introduce myself and the purpose of the interview thereby setting the stage.	Hello, my name is Amber Branson. I am a Doctoral Candidate with Walden University. The purpose of this interview is to is to identify and explore effective strategies used by health care business managers to reduce data breaches. I am going to ask you nine questions to which I would like your responses to. Then, I will conclude the interview. Do you have any questions?
Watch for nonverbal cues. Paraphrase the participant response. Ask follow-up probing questions to get more in depth	Interview questions: 1. What successful strategies have you implemented to prevent data breaches? 2. How did you measure the success of the strategy? 3. What challenges did you encounter when implementing the strategies to prevent data breaches? 4. How did you overcome the challenges? 5. What was the impact of the implemented strategy on profitability? 6. How would you describe the personal threat rating of the data breaches after implementing your successful strategies? 7. What other information regarding your successful strategies to prevent data breaches and sustain profitability that we have not already discussed would you like to share?

<table>
<tr><td>Wrap up the interview thanking participant.</td><td>Thank you for participating in the interview, an integral part of my research project.</td></tr>
<tr><td>Schedule a follow-up interview to perform member checking with the participant.</td><td>I will contact you in a week to schedule a time for us to review the accuracy of my interpretations of your interview responses.</td></tr>
<tr><td colspan="2">Follow-up Member Checking Interview


Graphic adopted from DBA Qualitative Pragmatic Inquiry Research handbook (2023). Not needed in proposal or research project. A visual reminder during proposal stage when creating interview protocol</td></tr>
<tr><td>Introduce myself and purpose of the follow-up interview to set the stage.</td><td>Hello,

Thank you for taking this time to meet with me again to review the accuracy of my interpretations of your interview responses.</td></tr>
<tr><td rowspan="3">Share a copy of the succinct synthesis for each individual questions.
Bring in probing questions related to other information that I found – note the information must be related so that you are I am probing and adhering to the IRB approval.
Walk through each question, read the interpretation, and ask: Did I miss</td><td>I will read the questions one at a time and my interpretations of your responses to them and ask you if my interpretation is correct.</td></tr>
<tr><td>1. Question and succinct synthesis of the interpretation—perhaps one paragraph or as needed</td></tr>
<tr><td>2. Question and succinct synthesis of the interpretation—perhaps one paragraph or as needed</td></tr>
</table>

anything? Or What would you like to add?	3. Question and succinct synthesis of the interpretation—perhaps one paragraph or as needed
	4. Question and succinct synthesis of the interpretation—perhaps one paragraph or as needed

Appendix B: Participant Invitation Template

There is a new study about reducing data breaches that could help health care business leaders better understand strategies used to engage employees and positively impact organizational performance. For this study, you are invited to describe your successful strategies to engage employees.

About the study:

- One 30–60-minute phone interview that will be audio recorded (no videorecording)
- To protect your privacy, the published study will not share any names or details that identify you.

Volunteers must meet these requirements:

- Business leader
- Employed at the organization in a position implementing data breach strategies for 24 months or more

The interview is part of the doctoral study for Amber Branson, a DBA student at Walden University. Interviews will take place during (to be determined).

Please reach out to email@email.edu to let the researcher know of your interest. You are welcome to forward it to others who might be interested.