

10-21-2025

Successful Cybersecurity Strategies for Protecting Consumer Data

Zylia Ortiz
Walden University

Follow this and additional works at: <https://scholarworks.waldenu.edu/dissertations>

This Dissertation is brought to you for free and open access by the Walden Dissertations and Doctoral Studies Collection at ScholarWorks. It has been accepted for inclusion in Walden Dissertations and Doctoral Studies by an authorized administrator of ScholarWorks. For more information, please contact ScholarWorks@waldenu.edu.

Walden University

College of Management and Human Potential

This is to certify that the doctoral study by

Zylia Ortiz

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. Jodine Burchell, Committee Chairperson, Doctor of Business Administration Faculty

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

Walden University
2025

Abstract

Successful Cybersecurity Strategies for Protecting Consumer Data

by

Zylia Ortiz

MS, Nova Southeastern University, 2005

BS, University of South Florida, 2002

Qualitative Pragmatic Inquiry Business Research Project Submitted in Partial Fulfillment
of the Requirements for the Degree of
Doctor of Business Administration

Walden University

November 2025

Abstract

The continued advancement of information technology, although extraordinary and innovative, may have a profoundly negative impact on the adequate protection of consumer information. Consumers and organizational stakeholders alike are increasingly concerned about the risk of data ending up in the hands of cybercriminals. Grounded in the routine activity theory, the purpose of this qualitative pragmatic inquiry research project was to identify and explore the strategies information technology leaders use to protect customer data from security breaches. The participants were eight information technology leaders in the Washington, D.C., Virginia, and Maryland area. Data were collected using semistructured interviews and public websites. Through thematic analysis, four major themes were identified: (a) employee training and consumer awareness, (b) development of security tools and capabilities, (c) cyber insurance and security compliance, and (d) securing financing and costs. One key recommendation is for information technology leaders to provide robust security training and knowledge management tools for both consumers and employees, as well as allocate a substantial budget for the development and implementation of security solutions. The implications for social change include the potential to lower the number of identity theft and security breaches, which can strengthen organizational security and help protect consumers' sensitive information.

Successful Cybersecurity Strategies for Protecting Consumer Data

by

Zylia Ortiz

MS, Nova Southeastern University, 2005

BS, University of South Florida, 2002

Qualitative Pragmatic Inquiry Business Research Project Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

November 2025

Dedication

First and foremost, I thank God for His constant presence, grace, and guidance throughout this journey. Without His strength, wisdom, and provision, I would not have reached this point. Every challenge, breakthrough, and late night has been marked by His faithfulness, and I am truly grateful.

To my son, you have been my greatest source of strength and inspiration. Your joy, patience, and loving presence carried me through the most challenging moments of this journey. Thank you for reminding me of what truly matters. This is dedicated to you—may it serve as a testament that with faith, determination, and perseverance, no dream is beyond reach. Always keep God first in all that you do. I love you, son!

Mom and Dad, thank you for your steadfast support, unconditional love, and enduring belief in my potential. Your encouragement sustained me through moments of doubt and gave me the foundation upon which this achievement was built. I hope I've made you proud—this accomplishment is as much yours as it is mine. Love you!

To my family and those cherished friends who are like family, your unwavering love and support have been my anchor. Thank you for walking beside me on this long and rewarding journey. I love you all!

Acknowledgments

I am also sincerely thankful to my professor, Dr. Jodine Burchell, for her support, encouragement, and insightful guidance throughout this process. Your patience and honest feedback helped me grow both as a researcher and as a thinker.

Table of Contents

List of Tables	iii
Section 1: Project Foundation.....	1
Background of the Problem	1
Business Problem Focus and Project Purpose	2
Project Research Question	3
Assumptions and Limitations	3
Assumptions.....	3
Limitations	4
Business Project Ethics.....	4
Evidence-Based Integrative Review	6
Application to the Applied Business Problem.....	8
Conceptual Framework.....	8
Business Problem Scholarship Evidence	13
Business Topic Scholarship	17
Summary	28
Section 2: Primary and Secondary Industry Data Analysis	29
Nature of the Project	29
Method and Design.....	29
Reliability.....	30
Population, Sampling, and Participants	30
Data Collection Activities.....	31

Data Organization and Analysis Techniques	33
Summary	36
Section 3: Data and Professional Practice	37
Project Results	37
Presentation of the Findings.....	37
Theme 1: Employee Training and Consumer Awareness.....	38
Theme 2: Development of Security Tools and Capabilities	41
Theme 3: Cyber Insurance and Security Compliance.....	44
Theme 4: Securing Financing and Costs	47
Business Contributions and Recommendations for Professional Practice	51
Implications for Social Change.....	53
Recommendations for Future Study	55
Conclusion	56
References.....	59
Appendix A: Interview Protocol and Interview Questions.....	71
Appendix B: Interview Protocol	72

List of Tables

Table 1. Summary of Data Analysis ($N = 8$) 388

Section 1: Project Foundation

Background of the Problem

As technology evolves and advances, organizations find it easier to sell their products and services, and consumers can make purchases with the click of a button. This consistent advancement of technology has resulted in an exponential increase in the amount of data generated (Al-Zahrani & Al-Hebbi, 2022). While this advancement has put consumers eons away from the old days of making purchases in person, it also comes with risks. Studies have shown that the amount of data collected in 3 years exceeds what has been collected in the past 400 years, which is identified as big data and can be structured or unstructured (Al-Zahrani & Al-Hebbi, 2022). Big data can help generate revenue, improve the services offered, inform strategic choices, and more (Al-Zahrani & Al-Hebbi, 2022). Organization leaders should implement measures to protect customer data, including data policies that necessitate the development of more advanced strategies and protocols to safeguard customer information, whether collected on a website or application or consumer information stored in an organization's database.

An area that may provide additional protection for consumers is the implementation of federal regulations. The U.S. government is not implementing legislation to protect consumer data, and data brokers and organizations can gather and sell your data as they see fit (Martin, 2020). The absence of regulation leads to a lack of consumer trust in organizations that collect consumer data, given the numerous data breaches that have occurred (Martin, 2020). Unfortunately, individuals seeking to steal information or cause harm are increasingly finding new and advanced methods to gather

data from these transactions. In other words, they advance in tandem with technological advancements. Therefore, organizations must implement techniques to protect consumer data to gain customer trust and improve their profits.

Business Problem Focus and Project Purpose

The specific business problem was that some information technology (IT) leaders lack strategies to protect their customer data from security breaches. Therefore, the purpose of this qualitative pragmatic inquiry research project was to identify and explore effective strategies IT leaders use to protect customer data from security breaches. The target population included IT leaders. I employed a purposive sampling strategy to include eight IT leaders in the Washington, D.C., Virginia, Maryland area. The inclusion criteria for the IT leaders were that they must lead or supervise at least three employees and have demonstrated successful strategies to protect customer data from security breaches. I created an interview protocol to conduct semistructured interviews with the participants (see Appendix A). I also searched for public documents related to customer data security best practices, governance, policies, and procedures.

A qualitative methodology was employed in this research project. This method enables researchers to understand the interviewees' thoughts and feelings better as they relate to a specific topic (Quartiroli et al., 2017). The qualitative approach provided a clearer understanding of the successful strategies employed by IT companies to protect customers from security breaches.

I used a pragmatic inquiry design for this research project. The pragmatic inquiry design begins with an uncertain situation where problems are identified and explored

(Hartmann et al., 2015). Researchers then develop ideas for solutions to the problem and perform studies to determine what will work best (Hartmann et al., 2015). A pragmatic inquiry design was suitable for this research project because the pragmatic approach necessitates practical knowledge and rigorous research. This design is essential for IT leaders to identify and implement factual and valuable solutions that address organizational security concerns.

I analyzed the data using thematic analysis and methodological triangulation. I used the Delve Tool Software to analyze the interview transcripts made from the audio recordings. I coded the transcript data, categorized the resulting codes, and analyzed the categories to create themes.

The theory that grounded this study was the routine activity theory (RAT) created by Lawrence Cohen and Marcus Felson in 1979. They asserted that criminals and victims connect in time and space based on factors, such as motivated offenders, capable guardianship, and attractive targets (Guerra & Ingram, 2022). This framework offered an important perspective for analyzing how routine patterns influence criminal behavior.

Project Research Question

What effective strategies do IT leaders use to protect customer data from security breaches?

Assumptions and Limitations

Assumptions

According to Ransom et al. (2023), assumptions are the weight of evidence learned from samples and how it relates to the observer's perception of the generation

process of the sample information. I assumed that potential participants would answer each interview question honestly, based on their personal knowledge, experiences, and successes. Another assumption was that the participants were willing to contribute and take part in the study. An additional assumption was that, with today's technology, conducting interviews via video call would be sufficient to capture the required information. I addressed these assumptions by building a rapport with the interviewees.

Limitations

According to Rietdijk and Dräger (2024), a limitation occurs when factors significantly impact the results and hamper the external validity of the information collected or provided. The first limitation of the study was that technology is constantly evolving and changing. Security breaches will occur in different ways as technology continues to advance. Another limitation was that the participants were not local to my area; therefore, I was not able to conduct in-person interviews because travel to the location was prohibitive. I mitigated this by providing the option to do a video call.

Business Project Ethics

The role of the researcher in data collection is crucial. The researcher must communicate efficiently because it is a fundamental part of the research process (Harerimana et al., 2024). Communicating effectively allowed me to collect the data needed to complete the research, which included semistructured interviews with an interview protocol (see Appendix A.) I conducted this qualitative research project to identify and explore effective strategies for protecting consumer data from security breaches. This information would be helpful to IT leaders seeking different ways to

protect their consumer data while continuing to operate the business profitably and maintain consumer trust. With a background in cybersecurity and IT project management, I possessed relevant experience in engaging with IT leaders on data protection strategies. This shared professional experience helped build rapport, though I remained mindful of potential biases stemming from my own perspectives and took care to approach the data with a thoughtful mindset, allowing the participants' experiences and insights to shape the findings.

As the researcher, I ensured that all participants were treated with respect, fairness, and equity. According to the *Belmont Report*, there are three basic ethical principles: (a) respect for persons, (b) beneficence, and (c) justice (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979). Everyone participating in a research project should be treated with respect, mainly because their participation is voluntary. According to the U.S. Department of Health and Human Services (1979), all efforts should be made to ensure that participants are treated ethically and protected. Participants should always be treated equally and fairly (U.S. Department of Health and Human Services, 1979). By following these ethical guidelines, I ensured that all participants were treated fairly, with respect, and protected throughout the research process.

Once I received approval from the Walden University Institutional Review Board (IRB), I contacted potential participants. I utilized my professional network to identify individuals interested in participating in the research project. I contacted potential participants via email or phone to schedule a time to discuss the research project, assuring

them their information would be kept confidential, that codes would be used instead of their names in the study, and that the collected information would be securely stored for 5 years in my Google Drive. An IRB Consent Form had to be read, signed, and returned to me via email before an interview was conducted with a participant. No incentives were given to the participants; however, I reiterated my appreciation and the importance of their participation. I answered any questions or concerns they may have had and provided them with the IRB approval number (01-03-25-0056028). If they were interested and I had gained their commitment to the process, I proceeded with scheduling the audio-recorded interviews.

The participants were free to withdraw from the project at any time. However, I requested that they provide as much advanced notice as possible to avoid impacting the research and timeline. This also allowed me time to seek an alternate participant. I asked that the participants contact me by phone, email, or text to let me know if they no longer wished to participate in the research project.

Evidence-Based Integrative Review

This professional and academic literature review centered on the study's overarching research question with which I aimed to identify and explore effective strategies employed by IT leaders in securing customer data. In this integrative review, I sought to analyze and synthesize the extant information on the topic so that readers can understand the importance of obtaining consumer information and comprehend its daily impact on consumers and organizations.

The literature review is organized in the following order: (a) implementing regulations and policies on a federal and organizational level, (b) prevention of information security breaches, (c) IT strategies to protect consumer data, and (d) previous research supporting this study. The specific business problem was that some IT leaders lack strategies to protect their customer data from security breaches.

The integrative review involved a critical evaluation and examination of articles relevant to the project from the following databases accessed through the Walden University Library: ProQuest, EBSCOhost, Sage Journals, ResearchGate, and Google Scholar. These databases were searched to explore academic journals, articles, and relevant materials. I used the following keywords as part of a comprehensive search for this doctoral study: *routine activities theory, securing customer data, secure data strategies, protecting data, strategies, security, protecting consumer data, prevention of information security breaches, prevention of security breaches, protecting customer data, security breach, and consumer data*. I referenced a total of 43 sources and 42 peer-reviewed journals. Among these sources, 27 were published within the last 5 years, while the remaining 16 were published more than 5 years ago. Ninety-seven percent of the sources included in the study were peer-reviewed articles. I conducted this project to identify the need for effective strategies to secure customer data, explore how IT leaders have successfully protected their customer data, and outline the implementation of successful strategies that have prevented security breaches.

Application to the Applied Business Problem

In this qualitative, pragmatic inquiry, I explored the successful strategies IT leaders have used to protect customer data from security breaches. Consumers use technology for its various conveniences as technology continues to grow and evolve; however, these conveniences allow customer data to be stolen or exploited. The internet has provided numerous benefits, but it also carries the risk of data breaches for malicious intent (Prastyanti et al., 2021). Protecting consumer data is a significant problem that needs to be addressed. Data protection implies that consumers can determine how, when, and where their information will be used; however, once that information falls into the wrong hands, there is no way to determine how it will be used (Prastyanti et al., 2021). Therefore, identifying effective data protection strategies is critical for IT leaders to mitigate security breaches and maintain consumer trust in a quickly evolving digital landscape.

Conceptual Framework

The conceptual framework for this research project was RAT. RAT was introduced by two well-known criminologists, Cohen and Felson (1979). It is the most prevalent victimology theory of the last 40 years (Perkins et al., 2022). In RAT, Cohen and Felson hypothesized that crimes happen when three explicit components come together simultaneously: motivated offenders, suitable targets, and the absence of guardians against a violation. In other words, there must be an interested criminal, an attractive victim, and no protector present to prevent the crime from occurring (Guerra & Ingram, 2022). RAT drew attention to the increase in crime after World War II that was

attributed to the rise in opportunities for criminal acts (Maloku et al., 2024). Cohen and Felson stated that U.S. routine behaviors changed as more women entered the workforce outside the home and modern technology began to take over (Perkins et al., 2022). The changes provided more opportunities for offenders to commit crimes and eliminated the guardianship that had previously prevented crimes from occurring (Perkins et al., 2022). An advantage of this approach is that it helps connect crimes that previously seemed unrelated (Cohen & Felson, 1979). Researchers extended the phrase “motivated offender” to “being in the vicinity of the motivated offender” and “being exposed to risky situations” based on the frequency of internet use (Lee et al., 2022, p. 183). A suitable target was defined as the appropriateness of the target to the offender, based on the types of activities in which they participated (Lee et al., 2022). A capable guardian was defined as online security management (Lee et al., 2022). Overall, RAT helped me explain how changes in daily routines and technology use have created new chances for crimes to occur, especially online.

RAT is a straightforward and effective method. If the number of motivated offenders, or even viable targets, is to remain constant in a community, modifications in routine activities could alter the likelihood of their meeting in specific spaces and times, which would then increase the opportunities for crimes to occur (Cohen & Felson, 1979). This suggests that control is essential, and if control through routine activities declines, then an increase in illegal predatory activities can be expected (Cohen & Felson, 1979). It is akin to the time when the internet first emerged, with no laws governing its use. As

people began to use the internet to engage in destructive or harmful activities, more regulations were introduced to prohibit these actions.

Consumers now rely on online communications to conduct business, complete financial transactions, communicate with each other, and shop; however, these conveniences bring significant risks (Guerra & Ingram, 2022). With increased routine activities, crime is likely to rise, as individuals take advantage of these new opportunities. Interestingly, the increase in conveniences and benefits coincides with a rise in crime rates (Cohen & Felson, 1979). For instance, Leroy Gould demonstrated that the expansion of money circulation and the increased availability of automobiles between 1921 and 1965 led to a rise in car thefts and bank robberies (Cohen & Felson, 1979). Although society benefits from technology, it also means an increase in crimes and illegal activity that exploit these conveniences if not adequately guarded. Online victimizations have continued to increase as people rely primarily on online transactions (Guerra & Ingram, 2022). The growing reliance on online activities increases opportunities for criminals to exploit these conveniences, highlighting the need for stronger protections against digital crimes.

Monitoring how potential victims operate daily generally helps criminals, even cybercriminals. RAT has significantly influenced the growth of criminology, explaining the existence of criminal behavior and the increase in criminal acts (Maloku et al., 2024). People have routines that they follow every day, whether they are students, professionals, or retired. These activities can be related to economic means, family, education,

communication, or recreation (Maloku et al., 2024). Crime is deemed a disorderly behavior that conflicts with social norms.

Initially, RAT was used to explain variations in crime trends, but it later evolved to regulate, define, and prevent criminal activity. According to Maloku et al. (2024), RAT aligns with environmental criminology, which concentrates on the significance of opportunity. Today's technological advancements will continue to provide opportunities for bad actors to steal data and information. RAT has influenced law enforcement practices and prevention strategies (Maloku et al., 2024). The use of RAT to solve crime remains relevant today because it focuses on the motivation behind the criteria that lead to the offense.

The internet has opened the world to consumers, educators, retailers, bankers, and, unfortunately, cybercriminals. In relation to RAT, cyberspace has suitable online targets, exposure to online motivated offenders, and capable guardians (Puente & Hernández, 2022). An appropriate online target is the behavior of any internet user online. An online-motivated offender would exploit and target internet users and their online activities, while a capable guardian is a person or technical tool to prevent cybercrime (Puente & Hernández, 2022). Regarding social networks, users have risky behaviors that make them susceptible to victimization by motivated offenders (Puente & Hernández, 2022). Cyberspace is a vast platform for cyber victimization to continue to flourish, and it will get worse if no change is made.

A simple way to get access to people and organizations is online. The distribution of malicious spam is a common form of technical abuse (Perkins et al., 2022). Estimates

have indicated that spam accounts for over 281 billion emails sent daily; although it is often considered an irritation, this is typically how victims and offenders are connected (Perkins et al., 2022). Cybercriminals earn about \$200 million per year from spam distribution, and only 1 in 25,000 spam emails must be successful for a cybercriminal to make a profit (Perkins et al., 2022). Spammers who advertised medications also grossed \$2.7 million from false sales (Perkins et al., 2022). Alex Kirgel discovered that wealthy nations with high internet usage generated more spam than less wealthy countries and that a country's routine activities contributed to the distribution of spam in that country (Perkins et al., 2022). Studies have also shown that the more hours spent online, the more susceptible the person is to become a cybercrime victim (Perkins et al., 2022). RAT is a powerful approach for identifying patterns of cybercrime victimization (Perkins et al., 2022). This type of tool or solution is crucial in preventing bad actors from successfully stealing others' information.

RAT focuses on the factors that lead to a crime, emphasizing the offender, the victim, and the actual situation (Cohen & Felson, 1979). When attempting to solve a crime, these components would not hold much significance separately, but when viewed together as interconnected elements, they can lead to a meaningful resolution (Maloku et al., 2024). The goal is to understand and address the underlying conditions contributing to criminal behavior. By focusing on the conditions of criminal acts (i.e., motivated perpetrators, lack of social control, and the influence of place and time), the theory offers an inclusive approach to lowering crime rates (Maloku et al., 2024). RAT highlights that reducing crime requires addressing three key factors: reducing the motivation of

criminals, making targets less attractive to potential offenders, and improving the ability of guards to protect these targets (Maloku et al., 2024). Ultimately, RAT provides a practical framework for crime prevention by targeting the situational dynamics that facilitate criminal acts.

Business Problem Scholarship Evidence

Preventing data breaches is a common issue in most organizations. Cybersecurity refers to the protection of devices, data, and networks from unauthorized use and exploitation, and it is critical because many risks arise from inadequate cybersecurity protections, such as data breaches (Kempton, 2023). Cybersecurity is the activity or capability of protecting information and communication systems against damage, unauthorized use, illegal alteration, or misuse (Shaikh & Siponen, 2023). A data breach exposes protected or sensitive information to unauthorized individuals, potentially affecting any person, company, or organization that utilizes technology (Kempton, 2023). A data breach can negatively impact the confidentiality, integrity, or availability of an information system as mandated by security regulations or methods (Shaikh & Siponen, 2023). Some examples include phishing, denial-of-service attacks, zero-day exploits, ransomware, and unauthorized access to information systems (Shaikh & Siponen, 2023). The costs for the organization can be prohibitive. Data breach costs can include customer reimbursement, lawsuits, loss of market value, loss of investments, regulatory fines, blackmail payments, and the cost of lost business (Shaikh & Siponen, 2023). In 2020, approximately 45% of organizations in the United States experienced a data breach, and over the past decade, 15 billion data records have been compromised. (Kempton, 2023).

In this evolving world and its ongoing technical modernization, data breaches have negative impacts, including financial loss and a loss of trust (Kempton, 2023). As data breaches continue to pose escalating financial, operational, and reputational risks, it is imperative for organizational leaders to adopt comprehensive, proactive cybersecurity strategies that align with overall business objectives and foster long-term trust with consumers.

Organizations must prioritize securing their systems against cyberattacks and data breaches. U.S. corporations are the most vulnerable targets of data breaches and have generally responded to growing cyberattacks by placing a greater emphasis on strengthening cybersecurity as a defense (Kempton, 2023). Data breaches began in the 1980s, coinciding with the emergence of home computers, although they were not yet very complex (Kempton, 2023). This changed in the 2000s with the advent of mobile phones and laptops. A significant data breach occurred at Yahoo in 2013, where hackers accessed 3 billion accounts (Kempton, 2023). As cyber threats continue to evolve in scale and sophistication, it is critical for organizations to adopt forward-looking cybersecurity strategies that not only defend against current risks but also build resilience for emerging digital challenges. As cyber threats continue to evolve in frequency and complexity, it is critical for organizations to adopt proactive cybersecurity strategies that not only defend against current risks but also build resilience for emerging digital challenges.

Cybersecurity risk management is a tool that companies can use to mitigate data breaches. The cybersecurity risk planning and management process comprises four categories: deterrence, prevention, detection, and remediation; these are stages that an

organization should take before a breach is detected (Shaikh & Siponen, 2023). By carefully following these steps, organizations can establish a robust system to safeguard against cyber risks and maintain efficient operations over time.

The collection of substantial data has become increasingly popular in recent years, as people continue to enjoy the conveniences and innovations of technology. This data needs to be effectively stored with the ability to share the information, which has led to the rise in the use of cloud storage. Reports have indicated that 73% of reported security events occur more frequently in the cloud than on-premises IT systems (Li et al., 2024).

Organizations must stay current with known vulnerabilities and application updates to ensure the latest patches are implemented and to implement additional safeguards as needed. Organizations worldwide have witnessed the consequences of weak security policies and the rapid expansion of the technology industry because companies continue to experience data breaches despite efforts to implement cybersecurity within their systems (Kempton, 2023). Organizations must identify and mitigate risks as early as possible before they become a significant problem. IT departments must understand the various technology infrastructures and take precautionary measures to prevent data breaches (Kempton, 2023). Unfortunately, many companies have traditionally concealed data breaches to avoid public criticism and potential federal or civil charges. According to a survey of security experts, it is estimated that over 20% of companies have concealed a breach (Kempton, 2023).

Government entities are in place to hold companies accountable for data breaches, including the Federal Trade Commission (FTC) and the Securities and Exchange

Commission (SEC). The FTC is a federal agency that has led data breach investigations for over 50 years with the purpose of protecting Americans' privacy and establishing precedents to safeguard them adequately (Kempton, 2023). The FTC asserts "that an act by a company is considered unfair if it is likely to cause substantial injury to consumers, is not reasonably avoidable by consumers, or is not outweighed by benefits to consumers or competition" (Kempton, 2023, p. 2). They also passed the first federal privacy law, the Fair Credit Reporting Act, "which protects the privacy of consumer information contained in files from consumer reporting agencies" (Kempton, 2023, p. 3). The FTC is the principal federal office where companies must report data breaches and cyber issues to the government (Kempton, 2023). The SEC employs a different approach to managing data breaches. They focus on confirming that markets are impartial for all customers and give oversight for regulating the securities markets. Oversight includes policing cybersecurity-related business actions for organizations (Kempton, 2023). In the case of the *FTC vs Equifax*, the private information of approximately 147 million people in the United States was compromised in 2017 (Kempton, 2023). Equifax failed to implement fundamental security measures, and subsequently, the organization and its executives were held accountable when the FTC and SEC investigated the matter (Kempton, 2023). The FTC concentrated on holding the entire organization accountable by requiring that it pay out \$575 million. The SEC investigated executives who were aware of the breach and engaged in insider trading before the breach was publicly announced (Kempton, 2023). Consumers typically do not see how an organization's cybersecurity operations

work; they invest their money, assuming everything is in order. The SEC fills the gap by monitoring companies' cybersecurity controls (Kempton, 2023).

The Internet of Things (IoT) technology is key when discovering solutions to reduce or prevent data breaches. The IoT technology constantly connects to the internet, global positioning systems, processors, and more (Balakrishnan et al., 2021). The constant connection increases the opportunity for a cyberattack or cyber threat. The IoT networks should be improved, and device manufacturers should apply security protocols (Balakrishnan et al., 2021). Threats, such as spoofing and denial-of-service attacks, utilize wireless networks for their exploits, stealing information and controlling the devices connected to them. Attacking an available IoT platform would not be challenging for hackers because the primary advantage of the IoT is its ease of connection to both hardware and software (Balakrishnan et al., 2021). The IoT is a new technology, but its security and privacy are inadequate. Several processes, procedures, and systems can secure a network; however, systems are still vulnerable to breaches (Balakrishnan et al., 2021).

Business Topic Scholarship

Implementing Regulations and Policies on a Federal and Organizational Level

A customer's data must be protected on a federal level by implementing regulations, policies, and organizational standards. Personal data are defined as any information that is connected to a person who is identified or could be identified, either directly or indirectly, including information, such as their name, ID number, location, online username, or details about their physical, mental, financial, cultural, or social life

(Martin, 2020). The internet is used for making financial transactions, trading, shopping, and health services, and organizations collect this data. With the increasing use of the internet, the most effective way to protect consumer data must be determined (Prastyanti et al., 2021). The increased use of technology in people's daily lives has had a tremendous impact on the amount of consumer data being collected and stored. The risk of breaches, ransomware, and compliance violations has been exacerbated by unrestricted data collection (PR Newswire, 2021). The risk is not in stopping consumers from providing information but in not stopping the collection of this data. Organization leaders struggle to find efficient methods for collecting, analyzing, and securely storing consumer data (PR Newswire, 2021). IT leaders have stated that data are being amassed in unofficial repositories, like email and local devices, and ransomware is currently the most considerable burden from the perspective of access and exposure of the organization's data, with smaller businesses not having the capital to implement a proficient and effective security solution (PR Newswire, 2021). IT leaders have found that data are often stored in unofficial and unauthorized storage, such as email, portals, and local mechanisms (PR Newswire, 2021). A significant threat is ransomware, along with the impacts that result from the exploitation of vulnerabilities (PR Newswire, 2021). Factors, such as the limited resources of small businesses and the emergence of artificial intelligence (AI), are emerging as significant security concerns with substantial implications for consumer data security (PR Newswire, 2021).

Industry regulation is imperative in every industry to protect consumers from various perspectives, including financial, environmental, medical, data privacy, and the

abuse of power. People can be exploited for financial gain; therefore, implementing data protection laws is particularly important as the development and use of systems for trade, banking, and public services are operated and utilized by consumers (Prastyanti et al., 2021). Requiring organizations to comply with security regulations may motivate them to implement more effective strategies that protect data (Mustapha et al., 2023).

The FTC (2021) has implemented the Safeguards Rule, which requires mortgage brokers, payday advance companies, car dealers, and other nonbanking organizations to create, employ, and maintain methods to protect consumer information. Specifically, they need to minimize access to consumer data and utilize encryption to protect it (Federal Trade Commission, 2021). The FTC also implemented the Gramm-Leach-Bliley Act rule, which requires financial institutions to inform customers about how their information is shared and to provide them with the option to opt out of information sharing.

Congress should enact regulations and legislation mandating that organizations adopt practices to safeguard consumer data and impose penalties for inadequate data protection. Data brokers are a primary offender in the exploitation of consumer data. Congress should impose requirements that notify consumers of how their data is used, provide them with a choice to opt out, and offer access to the information, allowing consumers to edit it as needed (Martin, 2020). Currently, no federal regulation prevents companies from using consumer data for marketing purposes, and most consumers are unaware of this (Martin, 2020). The European Union has implemented the General Data Protection Regulation, and other countries should follow suit. This regulation provides

online privacy for consumer data and data collection (Martin, 2020). No federal regulation in the United States covers consumer data collection. Some regulations protect certain types of information, like the Fair Credit Reporting Act for credit information, Health Insurance Portability and Accountability for medical information, Gramm-Leach-Bliley Act for financial information, and Children's Online Privacy Protection Act for children's information; however, none covers consumer data protection for marketing purposes (Martin, 2020).

Consumers need to be protected from those who seek to harm. The National Telecommunications and Information Administration has taken the initiative to protect consumer data and has requested input from major corporations in the industry and consumers (Martin, 2020). The major corporations agreed that federal regulation was the most effective way to protect consumer data; however, the consumer side stated that the information was too vague and wanted more details (Martin, 2020). The Electronic Privacy Information Center suggested that a federal standard be developed, allowing each state to determine more precisely what was best for them (Martin, 2020). There is a push from all groups, but this must be addressed as technology continues to advance.

Consumers should be aware of where their information is stored, how it is used, and by whom. Data will always remain vulnerable without established rules, legislation, and/or regulations. Consumers should be given notice when their information is being shared, a choice as to whether they want it shared, and an option to update erroneous data as needed (Martin, 2020). An alternative approach to protecting consumer data is to standardize the amount of data an organization collects (Martin, 2020). Firm penalties

should be imposed on organizations that refuse to comply with the regulations (Martin, 2020).

In some organizations, software developers are specifically hired to engineer ways to target specific demographics. Some automated systems are discriminatory and biased, and there are instances where social media platforms monetize youth data (James, 2023). The Attorney General of New York has released a guide to help organizations protect consumer data (James, 2023). James (2023) recommended that organizations should implement nine key recommendations to protect consumer data:

1. It must maintain secure authentication controls by using secure methods, requiring strong passwords, and protecting those passwords from attacks.
2. Sensitive customer information should be encrypted, with backup protections and rules in place in case initial safeguards fail.
3. Organizations must ensure that any service providers they work with employ reasonable and adequate security measures to protect consumer data.
4. It is important to know precisely where consumer information is stored, so that all data can be adequately secured.
5. Companies should guard against data leakage in web applications by ensuring that sensitive information is encrypted and hidden when transmitted online.
6. In the event of a data breach, organizations must take immediate steps to protect any affected customer accounts.

7. Unnecessary or inactive accounts, often referred to as "orphan accounts", should be deleted or deactivated because they can provide entry points for hackers.
8. Companies should guard against automated attacks, such as credential stuffing, which involve repeated login attempts to gain unauthorized access.
9. Consumers should be given clear and accurate notices about how their data are used and protected, so they are fully informed about any potential risks or issues.

These are areas where an organization can implement rules to protect consumer data and at least minimize data breaches (James, 2023).

Prevention of Information Security Breaches

Consumers have easy access to data at their fingertips. Consumer education and awareness are crucial for protecting their data; however, when consumers conduct business or transactions on an organization's website, they trust that their information will be secure. The business they conducted on the site has now made them vulnerable to becoming a victim of fraud. The increase in cybersecurity breaches has caused much concern among organizations' stakeholders (Boss et al., 2024). The Institute of Internal Auditors and Information Systems Audit and Control Association stated that the top organizational threat is cybersecurity (Boss et al., 2024).

One notable example of a significant security breach is the 2019 Capital One data breach. A software engineer gained access to their systems through a firewall that was not appropriately configured (Boss et al., 2024). This resulted in the illegal collection of

personal information from U.S. and Canadian citizens, costing the company between \$120 and \$170 million (Boss et al., 2024).

Another instance of the need to prevent security breaches is the 2017 breach at Equifax. The company failed to install the necessary security patch to secure its systems, which allowed hackers to access their systems and steal server data (Boss et al., 2024). There were 146.6 million names and birth dates, 145.5 million social security numbers, and approximately 200,000 credit card numbers stolen (Boss et al., 2024). This cost Equifax \$400 million, with an additional \$1.5 billion spent on enhancing its security systems (Boss et al., 2024).

A security breach that occurred at Target was particularly memorable because a top executive was fired in the aftermath of the breach (Boss et al., 2024). Hackers were able to gain access to their systems, download malicious software, and, unbeknownst to Target or its consumers, collect consumer data (Boss et al., 2024). Roughly 40 million credit card numbers had been stolen, which impacted about 110 million customers and cost Target \$291 million (Boss et al., 2024).

These examples illustrate the urgent need to enhance and secure information systems. As technological advancements continue to be created and enjoyed, security must be prioritized at the top. The IoT devices have become a great convenience and are used in healthcare, automation, and other fields. A technology that emerged to accommodate that technology is Wi-Fi-HaLow, which offers low power use and greater range abilities that is helpful in many different environments (Govindan et al., 2024). The advantages of IoT devices, such as low power consumption and reduced memory

requirements, are beneficial; however, this does not allow for resilient, vigorous security measures. Conventional security measures require heavy cryptography and intrusion detection that cannot be applied to an IoT device (Govindan et al., 2024). An efficient way to secure these devices would be to improve the port scanning process that would enable security administrators to identify vulnerabilities, allowing them to implement necessary measures to prevent their exploitation (Govindan et al., 2024).

These days, almost anything can be downloaded, from games to documents. Downloading applications from the internet and entering your data into them without understanding the associated risks is not a safe practice (Prastyanti et al., 2021). Educating users and ensuring they know the risks of sharing their personal information is another way to circumvent data security events (Mustapha et al., 2023). Developing educational security awareness programs for consumers and professionals that create these systems will help them be more knowledgeable in user creation (Mustapha et al., 2023).

IT Strategies to Protect Consumer Data

The first topic to be covered regarding the security of consumer data is big data. Big data can provide the necessary data to facilitate the development of effective data handling processes, such as product marketing, planning, financial management, and crucial efficiency (Muhasin et al., 2024). The use and study of it, along with its relationships, have helped strengthen data in the medical and industrial fields and have been integrated into their systems (Muhasin et al., 2024). However, securing big data is very difficult. Managing, accessing, sharing, and collaborating on data from diverse

entities and determining its relevance, is a significant challenge (Muhasin et al., 2024). Compromised sensitive information can be used to conduct an actual attack, which is why the primary goal of an organization is to use big data while also safeguarding the data and privacy. (Muhasin et al., 2024).

The more people shop online and use applications, the more information is being collected, which is referred to as big data. Big data results from the continued advancement of technology, comprising large amounts of data (Al-Zahrani & Al-Hebbi, 2022). This data represents a considerable amount of information typically used by organizations to inform their decisions; it can be structured or unstructured (Al-Zahrani & Al-Hebbi, 2022). The storage, processing, and transmission of this data require data security (Al-Zahrani & Al-Hebbi, 2022). Other areas of concern include cryptography, data sources, validity, categorization, monitoring, and data computation (Al-Zahrani & Al-Hebbi, 2022). The primary goal is to provide services while ensuring that data are secure from hacking and fraud (Muhasin et al., 2024).

Big data presents many challenges, and how to confront or resolve these issues vary. Some believe that data can be divided into three categories: (a) data, (b) process, or (c) system/management. Others believe that there is a fourth area, referred to as data quality and even fault system design, which is the issue (Al-Zahrani & Al-Hebbi, 2022). A layered architecture framework, known as the big data technology stack, was introduced by Nasser and Tariq (Al-Zahrani & Al-Hebbi, 2022). The layers are redundant physical infrastructure, security infrastructure, operational databases, organizing data services and tools, analytic data warehouses, and big data analytics (Al-Zahrani & Al-

Hebbi, 2022). Some studies have suggested that a viable solution is to consolidate vast amounts of data from multiple locations and store it in a single, secure, and regulated database (Muhasin et al., 2024).

A different area of thought is federated learning. Some believe that a decentralized technique, such as federated learning, is best because it enables groups to maintain autonomy over their intelligence data. Federated learning enables cooperative training across distributed networks while preserving the privacy of individual databases (Sakhare et al., 2023).

Decentralized trust management systems ensure the reliability and accountability of contributing organizations, which assuages the risks associated with centralized trust management systems (Velmurugan et al., 2024). If an organization leverages the power of cloud computing and decentralized trust management, it will achieve scalability, reliability, data integrity, and protection of shared data (Velmurugan et al., 2024). To improve security, they would incorporate decentralized trust management systems into cloud-based data-sharing frameworks, which would distribute trust management responsibilities and provide robust protection against unauthorized access and data breaches (Velmurugan et al., 2024). Utilizing the most current technological advances, such as AI and big data, while integrating data and providing value while protecting data and confidentiality is a challenging and critical task (Velmurugan et al., 2024). Access control tools are essential for resource sharing but protecting user privacy and managing permission changes present challenges. Offering a cloud-based decentralized trust management systems and an Efficient, Provably Secure Data Selection Sharing Scheme

is ideal. The Efficient, Provably Secure Data Selection Sharing Scheme cryptography and encryption techniques control access, ensure reliability and accountability, allow data owners to maintain control, identify shared data, and facilitate data merging, thereby reducing the amount of data (Velmurugan et al., 2024). This configuration would deter the impersonation of a cloud service provider, selective data forgery, and trust credential forgery (Velmurugan et al., 2024).

The lack of security in software applications is a significant contributor to the need for data protection. Consumers download applications to facilitate transactions, manage their finances, communicate with others, play games, and more (Mustapha et al., 2023). Some of these applications are easily exploitable by someone looking to collect data for malicious purposes. These threats can compromise user information, business transactions, and even the reliability of the application (Mustapha et al., 2023). To reduce these risks, organizations can implement user authentication procedures, encryption, and robust access restrictions (Mustapha et al., 2023). IT is an industry that requires continuous research to determine the most effective methods for protecting consumer data (Mustapha et al., 2023). Possible security solutions could be blockchain, the IoT, AI, or the acceptance of complex and varied processes and procedures (Mustapha et al., 2023).

Organizations are increasingly utilizing AI and machine learning to support informed decision-making; however, this has left these organizations more vulnerable (Dhabliya et al., 2024). Data protection is key to securing these environments. System resilience strongly relies on monitoring and anomaly detection, and strong incident

response is critical (Dhabliya et al., 2024). Protecting machine learning systems requires a comprehensive strategy that incorporates monitoring, incident response, model security, pipeline security, and data protection (Dhabliya et al., 2024). Support vector machines is an essential algorithm because it creates firm decision boundaries that protect from hostile attacks (Dhabliya et al., 2024). Random forest is capable of ensemble learning, which provides resilience against overfitting and data noise (Dhabliya et al., 2024). Considerations for integrating support vector machines and random forest can enhance system robustness (Dhabliya et al., 2024).

Summary

This integrative review comprised a comprehensive examination of academic literature on the strategies employed by IT leaders to safeguard consumer data. I also provided examples and covered the importance of preventing security breaches. The background of the problem, including security breaches, and the purpose of this research project were discussed in this section. Similarly, I highlighted the research projects's assumptions, limitations, and ethics. The section also contained a comprehensive exploration, analysis, and review of articles and studies related to security breaches, thereby expanding the existing coverage. Additionally, I provided the conceptual framework used and evidence regarding the need for and importance of the study. In this study, I examined the need to implement federal regulations and policies to prevent information security breaches and strategies that will protect consumer data. Securing the data that are input into devices and provided to organizations has been and continues to be extremely important.

Section 2: Primary and Secondary Industry Data Analysis

Nature of the Project

Method and Design

I decided to use the qualitative research method to conduct this in-depth examination of cybersecurity methods due to the alarming rate of growth and instances of security breaches. The qualitative approach is the best way to gain an understanding of one's views and explain their experiences (Elhami & Khoshnevisan, 2022).

Organizations have a crucial need to collaborate with academic researchers and specialists because data breaches have become increasingly complex (Nejjari et al., 2024). The solutions or strategies in place for security breaches are not a set standard; they vary from person to person. Every organization takes actions based on what is best for its company, its resources, and so on. Collecting data from IT leaders who work with security at various organizations enabled me to observe the diverse methods and strategies that have been successful for these organizations and their customers.

Qualitative research has suggested that understandings and practices can be fully expressed through a person's language, providing a solid representation of their experiences (Crowe & Manuel, 2025). The pragmatic approach can assist in resolving issues within organizations because it enables one to navigate the changes and complexities of the organization (Ambrož, 2024). The pragmatic inquiry design focuses on using clear ideas to explore real-world evidence, not because everyone believes in the same theory or philosophy, but because they are committed to understanding things through careful analysis (Benzecry et al., 2017).

Reliability

To ensure the reliability of this study, I followed a process of selecting the appropriate IT leaders to interview, asking relevant questions, and reviewing publicly available data to support the study further. Reliability refers to the quality of being trustworthy or dependable (Novosel, 2024). To ensure dependability and reliability, I requested participation in the study from IT leaders who were knowledgeable about their organization's security posture. I established a procedure that was used with every participant to ensure that I started the interview with the right questions. Every interview was audio recorded, transcribed, and then reviewed and analyzed using the strategies of member checking, data saturation, and triangulation.

Population, Sampling, and Participants

The participants for this study consisted of eight IT leaders who were executives in their organizations and had implemented successful strategies that protect their customer data from security breaches. I gained access to the participants through emailing invitations, LinkedIn connections, professional associations, and prior work colleagues. After the IT leader responded to my email, I would reach out to them and correspond to build a rapport, ultimately leading to purposeful, fact-based, and impartial research. We discussed our academic and professional experiences regarding the topic of this study. We also reviewed current events and discussed how trends could continue to evolve in the field, given the ongoing advancements in technology. This inspired them to participate in the research and share their knowledge and expertise.

I used purposive, expert sampling for this study. Purposive sampling focuses on specific characteristics that a participant must possess for the researcher to gather the exact information they are seeking (Campbell et al., 2020). This type of sampling suggests that certain types of professionals possess valuable knowledge and experience relevant to the research topic (Campbell et al., 2020). Purposive sampling occurs when a researcher selects a specific set of individuals to comprise the sample studied for the research (Spolarich, 2023). A subtype of purposive sampling is expert sampling. This is where the candidates are selected based on their expert knowledge or experience related to the research topic (Spolarich, 2023). I had eight participants who were willing to participate in this research project.

I found that data saturation was reached at the fifth interview. Data saturation is an essential aspect of qualitative research. There is no requirement for a specific number of interviews in qualitative research, but instead there is a focus on actual saturation (Christou, 2025). Saturation is reached when no further understandings, perspectives, or values emerge from additional interviews (Christou, 2025). It is about the depth of data collected from the study participants (Christou, 2025). I found that no new data or findings resulted from the interviews; however, to confirm, I conducted an additional three interviews to ensure that I had reached data saturation.

Data Collection Activities

I, the researcher, served as the primary data collection tool, collecting and analyzing data through virtual, semistructured interviews. Semistructured interviews produce precise data, which are ideal for investigating multifaceted and evolving

approaches (Brosnan et al., 2024). I explored various sources to identify candidates willing to participate in this study, including LinkedIn, professional contacts, and former colleagues. I assessed the candidates to determine if they would be able to contribute meaningfully to my research. Once I received consent for their participation, I scheduled a virtual interview. An interview protocol was used with each participant to bring some structure. The logic behind using an interview protocol was to ask questions specifically designed to gather information that would contribute to the study (Leong & Said, 2024). The interview protocol directed the interview regarding a specific subject and enriched my understanding of what the participants wanted to convey in the interview (see Leong & Said, 2024). I was able to ask supplementary questions based on the information that the participant provided. The interviews were audio recorded and transcribed using the Zoom application. I conducted member checking to ensure participants could validate and provide feedback, confirming that the information they intended to communicate was accurately recorded. I also collected derivative data from widely available sources.

I conducted the semistructured interviews virtually to collect information from participants. Conducting the interviews virtually eliminated the need for me, the researcher, to be in the same physical location as the participant. The semistructured interviews prompted answers to six open-ended questions, which allowed participants to provide as much information as possible without any limitations. I reviewed publicly available records and databases to obtain additional relevant data that would contribute to my research.

The use of an interview protocol helped outline the flow of the interview. I started the interview with an introduction that contained my name, the date of the interview, and the person I was interviewing. Then I asked them to introduce themselves and recorded that they were participating in the interview voluntarily. Follow-up questions were then asked so the participant could elaborate on the information being provided. Lastly, I thanked them for their time. Furthermore, I asked if they would agree to validate the transcript to ensure that all the information provided was conveyed as they intended. Moreover, the publicly available records and databases used were an additional source of information that substantiated my research.

Data Organization and Analysis Techniques

I used thematic analysis as the research design for this project, which enabled me to identify and understand the themes that emerged from this research. Thematic analysis is a method for organizing information into groups that focus on a specific topic (Shah et al., 2023). The data are sorted and translated into operational words, which are then translated into codes (Li et al., 2021). These operative words are apportioned into different groups (Li et al., 2021).

While conducting this research and the interviews, I kept a reflective journal where I documented my thoughts during each phase of the process. Reflective journal writing can serve as a tool for individuals to reflect on and evaluate their experiences, categorize their approach, and develop a plan for their next steps as the research progresses (Pinninti, 2024). Cataloging and labeling proved very valuable in assisting me to categorize considerations and contemplations as I went through the process (Langan,

2021). Cataloging is the process of organizing labeled information to present a structure to the labeling process (Langan, 2021).

After conducting the interviews, I used the transcripts to organize the information gathered into specific groups. I then used software to code the different keywords, which helped me develop corresponding themes and subsequently led to effective strategies.

This approach makes the evaluation more binding and effective because of its availability, comprehensibility, and tractability (Dawadi, 2020). There are six phases to achieve this goal. They are:

- Phase 1: Familiarization with the data: My work in cybersecurity and being a consumer has made the subject matter very important to me, and I recognized how this is a serious problem that should be addressed.
- Phase 2: Generating initial codes: This is the best way to organize data to lead to the development of themes.
- Phase 3: Searching for themes: This is where I was able to review the data and see the relationships within the data.
- Phase 4: Reviewing themes: This is a more in-depth evaluation of the themes developed in Phase 3.
- Phase 5: Defining and naming themes: In this phase, I cultivated the themes to categorize the account of each theme.
- Phase 6: Writing report: This is where I stated and described the results that were conveyed in the data collection.

Following these steps is crucial to ensuring that the analytical progression of the data yields an exceptional and superior study (Dawadi, 2020).

I assembled all my data, including documentation, interview recordings and transcripts, notes, and journal entries, into folders labeled by their respective sources. My participants were labeled IT leader (ITL) 1–8 (ITL 1, ITL 2, etc.). All the public documents (PD) were labeled PD 1–3. Interviews with participants were conducted using the Zoom application on the agreed-upon date and time. I used the Notepad software to transform the audio files into transcripts and analyze them properly. In qualitative studies, the researcher will request that participants review, update, and confirm the validity of the information collected; this process is known as member checking (Kullman & Chudyk, 2025). Participants can review and make any necessary revisions (Kullman & Chudyk, 2025). I used member checking to ensure that the participant provided the information they wanted to convey during the interview. Of the eight participants I interviewed, five sent back their feedback regarding the member checking summary.

I employed thematic analysis to carefully examine all the data collected during the research process. I found similar topics and ideas across all resources but also encountered a few anomalies. Anomalies can be utilized for further research as the industry continues to modernize and practitioners become increasingly innovative.

As I continued to conduct interviews, I began to approach data saturation. I planned to interview eight IT leaders and review three publicly available documents related to my topic. I estimated that this was an adequate number of participants I could interview and review before reaching data saturation. Data saturation occurs when the

researcher realizes they are no longer hearing or collecting new ideas, thoughts, or strategies (Christou, 2025). Once I acquired enough information to address the research question, I knew that I would not need to collect any further data (see Christou, 2025). Collecting, interpreting, and connecting all the information allowed me to answer the research question (Kawar et al., 2024). In addition to member checking, I employed triangulation to enhance the credibility and validity of the research findings.

Summary

In this qualitative, pragmatic inquiry research project, I explored IT leaders' successful strategies for protecting customer data from security breaches. Participants were IT leaders who had successfully implemented cybersecurity countermeasures to thwart cybercriminals from stealing or illegally accessing consumer information and who also resided in the United States. To collect data, I conducted semistructured, audio-recorded interviews with the participants as well as searched for and reviewed publicly available documentation that was related to this study.

Section 3: Data and Professional Practice

Project Results

The purpose of this qualitative, pragmatic inquiry was to explore and investigate IT leaders who have successfully implemented strategies to protect their customer data from security breaches. The research question was: What effective strategies do IT leaders use to protect customer data from security breaches? The challenge of securing cyberspace now extends beyond technological solutions, placing significant emphasis on the behavioral dimensions of cybersecurity. As home computers are increasingly utilized for remote work, professional development, and leisure pursuits, ensuring their security has become a matter of considerable importance (Arenas et al., 2024). During this study, I discovered common strategies that have been effective for various IT leaders across different industries and organizations: (a) employee training and consumer awareness, (b) development of security tools and capabilities, (c) cyber insurance and security compliance, and (d) securing financing and costs. All the themes contributed to the successful protection of consumer data in organizations and could truly assist other IT leaders in keeping their consumer data safe and secure.

Presentation of the Findings

I organized semi-structured interviews with eight IT leaders who have implemented security strategies in their respective organizations. I assigned each participant a unique code name: ITL 1 through ITL 8. The themes presented in Table 1 reveal a consistent pattern within the collected data and resonate with findings reported in the literature review in Section 2.

Table 1*Summary of Data Analysis Themes (N =8)*

Themes	Number of participants who contributed data to the theme	Number of excerpts from data assigned to the theme
Theme 1: Employee training and consumer awareness	6	69
Theme 2: Development of security tools and capabilities	7	39
Theme 3: Cyber insurance and security compliance	8	111
Theme 4: Securing financing and costs	8	33

Theme 1: Employee Training and Consumer Awareness

Employee training and consumer awareness are proven to be effective methods for protecting consumer data. One way IT leaders can enhance consumer data protection is to educate consumers on how to distinguish between genuine and fake emails and websites. Studies have shown that this type of training is highly effective (DeLiema et al., 2025). Evidence has suggested that sharing cybersecurity information and guidelines in a straightforward online tutorial may also help consumers develop greater confidence in their ability to identify phishing emails, which in turn will enable them to avoid imposter scams (DeLiema et al., 2025). Increasingly, research has highlighted the effectiveness of fraud education in protecting consumer data. Studies have shown that agencies and online retailers can help with this by adding this type of valuable information to their electronic communication methods (i.e., email, websites, etc.; DeLiema, et al., 2025).

ITL 1 emphasized the importance of training consumers and employees in the fight to protect consumer data, noting that one of the most crucial steps is to enhance the knowledge and understanding of individual users. They emphasized the importance of

reinforcing information and habit forming, so they know what to do when an attempt is made against the data they are charged with protecting. ITL 1 suggested that everyone should have “a general understanding of maintaining the security and integrity of their information. The consumer first must become much smarter regarding their information and how they release it.” ITL 3 mentioned that the use of a cybersecurity awareness program has been helpful in their organization. They stated, “It’s probably one of the huge things that I have done in both industries, made sure that there was annual security training for our end user community and an incident response and business continuity.” ITL 2 noted, “We do training from the top down, enforcing security emails and the importance of cybersecurity.” It is a requirement at their organization that training is completed annually. Their overall thought was to “provide them adequate training and then ensure you have your security measures in place.” ITL 8 said,

As far as the internal adoption, it’s education. The problem is people are afraid of what they don’t understand or know. So, I find educating the mass, especially with these new controls that we’re going to implement and put in place usually helps drive the adoption phase instead of just coming out and saying. You all have 3 months that you’re going to do this. Let’s take those 3 months first and go on a roadshow and educate everyone why we’re doing it, what they’re doing it for, and how it would help the business and organization. And then that kind of eases it in.

ITL 8 also mentioned, “I know that in this day and age, with the security issues that we are experiencing, just overall, I think the more educated consumers are, the better it will be for them.”

PD 2 discusses how many consumers today manage and organize their lives online (National Institute of Standards and Technology [NIST]-29, 2024). This can lead to issues with privacy and protecting data because data are being collected, used, stored, and shared by any organization that chooses to (NIST-29, 2024). This will continue to progress as technology advances. Governments around the world are beginning to address these issues by updating laws and implementing new regulations (NIST-29, 2024). The NIST has developed a privacy framework that enables organizations to manage their privacy risks and establish trust with consumers and their partners. Security breaches can also be used as tools in future planning and implementation. PD 2 states that logging and reporting features should notify all relevant members of their roles and alert the organization if further training on proprietary data distribution is needed (NIST-29, 2024). Not only should training be required regularly, but lessons also learned could provide additional opportunities to better secure systems and data going forward.

Theme 1, promoting employee training and consumer awareness, supports the current literature, which suggested that executives play a crucial role in implementing employee training programs, such as Security Education Training Awareness (Chin & Chua, 2021). Cybercrime has increased significantly over the last decade, primarily due to the rise of social media, online shopping, and online banking. Cybercriminals continually refine their tactics, seeking novel methods to exploit vulnerabilities within the digital landscape. To mitigate the risks associated with cybercrime, it is crucial to remain informed about emerging threats and implement robust cybersecurity measures (Panda et al., 2023). The schemes that cybercriminals continue to enhance and utilize persist

because of mistakes made by consumers, who are often unaware of the situation and lack adequate training (Panda et al., 2023). These days, it has become increasingly difficult for consumers to distinguish between genuine emails/information and fake emails/information. This has had a significant impact on both consumers and companies. Cybercriminals exploit these vulnerabilities in the environment to gain unauthorized access to sensitive data, including consumer information, financial details, and proprietary information (Panda et al., 2023). Organizations must be aware of these hazards and understand how they can harm their operations. They need to educate their employees about the risks of various cyberattacks (Panda et al., 2023).

This theme aligns with the RAT conceptual framework, in that consumers and employees can be trained in this theory, enabling them to understand and learn how to protect themselves or consumer data. As stated before, in RAT, it was hypothesized that crimes happen when three explicit components come together simultaneously: motivated offenders, suitable targets, and the absence of guardians against a violation (Cohen & Felson, 1979).

Theme 2: Development of Security Tools and Capabilities

There are many security tools and capabilities available to implement within an organization to protect consumer information. If these tools were not utilized, then all sensitive information would be vulnerable and at risk. Technology continues to modernize and advance, and with that also come the criminals and cyberattacks. Security solutions and implementations must be just as important as technological advancements.

If this does not happen, the bad actors will continue to exploit system vulnerabilities and steal consumer information.

Security tools, such as multifactor authentication, antivirus software, and firewalls, are crucial in protecting consumer data. Technology moves quickly, and industry and organizations need to keep up while also protecting their data. ITL 5 noted, “Some of the tooling we might use actually does help us keep up to some extent.” ITL 8 mentioned that the use of Application Program Interface (API) security in the cloud, which ensures that developers code securely from inception through the Continuous Integration and Continuous Delivery (CI/CD) pipeline in a DevSecOps environment, is very useful. ITL 7 addressed the utilization of specialized tools, such as Splunk, and their integration with established environments, including Amazon Web Services (AWS) and Azure, to strengthen security protocols. The interview underscored the significance of these tools in executing security strategies, supporting the relevance of the tools code. Additionally, ITL 7 details procedures for monitoring data security on servers and Elastic Cloud Compute (EC2) instances by outlining steps, such as evaluating customer-specific tools, validating integrations with cloud services, and implementing a 30- to 90-day performance review period. This systematic approach highlights the importance of continuous oversight and verification, aligning with the monitoring code. The inclusion of specific solutions, such as Terraform, for validating database information further emphasizes the participant’s dependence on these tools to ensure data integrity, which is consistent with the tools code.

The industry needs to implement various security tools to protect individuals from data breaches. PD1 mentions a solution that includes tools that automate data sensitivity detection, access controls for data, encryption, and multifactor authentication (NIST-28, 2024). Security tools that log information must be managed to ensure they collect only the necessary information to meet security requirements (NIST-28, 2024). PD 1 provides an example. Cisco Duo functions as a multifactor authentication (MFA) and single sign-on solution. In this project, Dispel manages access to internal systems via virtualization, while Duo provides an added layer of multifactor authentication between Dispel and the internal systems. This integration maintains robust access control by ensuring that, even in the event of a compromised Dispel virtual machine, there is still substantial protection between that environment and the enterprise's internal machines. PD 2 mentions how the integration of a logging capability could enhance the effectiveness of the tool by creating alerts, providing historical archives, and facilitating compliance initiatives (NIST-29, 2024).

Theme 2, the development of security tools and capabilities, supports current literature. For example, Acronis, a cybersecurity and data protection organization, conducted a survey that asked consumers about their top security concerns, their awareness of cyber risks, and the security measures they use to protect their personal information (Acronis Data, 2025). The results showed that 64% of the people surveyed identified data breaches as their top concern (Acronis Data, 2025). Forrester offers a data security and privacy playbook that outlines security tools to help organizations protect sensitive data from cybercrime and privacy risks through three steps: discover, plan, and

act (Abdullah, 2020). Companies can utilize this framework to advocate for the protection of consumer information within their organizations (Abdullah, 2020). There is also a tool called Sensing as a Service (S²aaS), which is a model that can be used for IoT (Bentahar et al., 2022). The cloud in S²aaS delivers public services via the internet and is designed to be scalable, interoperable, capable of managing large data sets, and minimizing maintenance requirements (Bentahar et al., 2022). S²aaS meets security requirements by ensuring transmission confidentiality, data integrity, service availability, system freshness, and mutual authentication among all IoT actors (Bentahar et al., 2022).

Theme 2, the development of security tools and capabilities, aligns with the RAT conceptual framework, where guardians are represented by security measures such as antivirus software, firewalls, and antispam solutions (Arenas et al., 2024). Information security management encompasses the deployment of security tools alongside the development and implementation of practices and procedures designed to safeguard information (Arenas et al., 2024). Security tools can detect and block potentially harmful files or activities before they have any impact (Arenas et al., 2024). Additionally, security tools automate scanning procedures, which help identify and remove malware that may exist on a system, thereby increasing process efficiency and reducing the required time (Arenas et al., 2024). Risky online activities increase the likelihood of a cyber-attack, aligning with the RAT.

Theme 3: Cyber Insurance and Security Compliance

Through my research, I have observed the importance of incorporating security into organizational and developmental IT plans. There has been a significant increase in

cyber risk over the past decade, and it continues to evolve (Joshi et al., 2025). There are several ways to mitigate this risk, and I focused on transferring the risk to cyber insurance and compliance (see Joshi et al., 2025). Some organizations turn to cyber insurance and compliance standards. To utilize cyber insurance effectively, organizations must ensure they are fully compliant with the necessary configurations and security controls. If they are not in compliance, they will be deemed negligent in implementing the required security controls and will not receive the organizational insurance benefits.

The participants in the current study use cyber insurance in their organizations and find it to be useful. ITL 2 stated that they are implementing security and access limitations along with cybersecurity insurance. They mentioned “if anything happens, then we have the insurance in order to help us to recover any data that’s been lost.” ITL 2 also mentioned the requirement for security compliance, noting, “We have to do certain things in order to make sure we're within compliance. They'll verify that, if we ask for any kind of help.” ITL 8 also discussed cyber insurance and security compliance, mentioning the issue surrounding the prevalence of ransomware today. Ransomware is a type of cyberattack in which criminals encrypt a system’s data and demand payment to restore access or avoid public exposure (Huang & Cornell, 2025). Insurance companies will help, but they will conduct an evaluation of your organization to ensure that the proper controls are in place (Adriko & Nurse, 2024). At times the insurer will require certain controls to be in place to receive coverage or may offer lower premiums if specific controls are in place (Adriko & Nurse, 2024). Security compliance is important for the company, but it is also crucial in the event of an incident that requires insurance.

For reporting and compliance requirements, PD 2 examines the configuration of a tool designed to forward logs to an on-premises solution. This system generates logs related to potentially malicious network activity, data departure from the network, and other relevant details that facilitate the early identification of confidentiality-related incidents (NIST-29, 2024). Integration with existing logging capabilities enhances the understanding of information from several tools, supports alert generation, and ensures the maintenance of historical archives for complete reporting and compliance (NIST-29, 2024). Implementing these tools and controls will not only help the organization protect consumer data but also ensure compliance with security standards.

Theme 3, cyber insurance and security compliance, support current literature. An organization's ability to follow protective security standards will allow it to protect consumer and organizational data. Investing in cybersecurity controls and cyber insurance is interconnected (Joshi et al., 2025). At a certain point, exclusively relying on cybersecurity controls to mitigate risk becomes cost-prohibitive, making it more economical to transfer the residual risk to a third party through insurance. Organizations can lower their insurance premiums by reducing insured risk via enhancements to their cybersecurity measures. Given the potential for consistent losses and the effects of cyber incidents across and within industries, investing in robust cybersecurity controls not only benefits individual organizations but also enhances social welfare by improving the overall level of cybersecurity for organizations and consumers alike (Joshi et al., 2025). Cyber insurance is a crucial tool for managing cybersecurity risks, providing operational and financial support in the event of incidents (Huang & Cornell, 2025). Insurers dispatch

expert teams to assess threats, coordinate responses, and negotiate ransom payments when necessary (Huang & Cornell, 2025). Furthermore, cyber insurance encourages higher security standards, raises awareness of risks, and supports investments in prevention and mitigation (Huang & Cornell, 2025). Recent trends have shown its role expanding from risk management to proactive monitoring and advising.

Theme 3, cyber insurance and security compliance, also aligns with the conceptual framework. The RAT was established to facilitate a more effective analysis of trends and patterns in criminal activity. Cyber insurance and security compliance align with RAT in that there is an upward trend in cyber-related activities in the economy (Huang & Cornell, 2025). Organizations are implementing secure technology solutions, and algorithms and other fortified technologies are being developed to reduce the probability of incidents or exploited vulnerabilities (Huang & Cornell, 2025). Insurance helps fill the security gaps that are presented by the growing number of ransomware attacks (Huang & Cornell, 2025). RAT is straightforward to use and helps inform crime prevention policies by highlighting key areas. Environmental design choices are made to reduce opportunities for crime (Piasecki et al., 2021). RAT provides valuable insight into the evolving threat landscape and highlights the significance of the human element in effective cybersecurity management (Piasecki et al., 2021).

Theme 4: Securing Financing and Costs

The choice of implementation types will require a strategic decision that depends on an organization's size, development workflows, security requirements, compliance obligations, and infrastructure preferences (Manolov et al., 2025). The costs associated

with implementing and maintaining an organizational security system can be substantial. An organization must ensure that it plans for and secures the necessary funding to implement security measures, which is important to safeguard the organization and its customers. Most companies view the bottom line as the critical component of business success, namely, profit. Small- and medium-sized enterprises are unable to afford the costs associated with implementing efficient and effective security. ITL 5 stated, “I get concerned because it’s harder for individual firms, like small businesses like myself, and even mid-sized businesses that might have 100 plus people to keep up with that because it does take investment.”

Obtaining the necessary funds and resources to implement required security solutions within an organization can be challenging without executive support. All the IT leaders mentioned that securing the cost or funding for security implementation is critical. ITL 8 said,

Sometimes getting support from that level, buy-in from that level, will release the funds. We make sure we go directly up to the COO, CEO, or whoever the main individual is, the lead of the organization, so they can understand exactly what we’re protecting.

ITL 7 noted:

There’s certain cost savings that we will always want to provide for a customer. So that’s really the number one thing. How much is this going to cost either per second, per day, per week, per month? And if the cost is low enough or if the cost is effective. Then we will submit it through a process.

Additionally, ITL 8 mentioned,

the cost aspect is really making sure that we, again, align the controls of what we want to implement to the business and make sure it meets the business mission or can actually either enhance the business mission or be a business enabler.

The PDs that I analyzed address the costs associated with security, both monetary and societal. PD 1 stated an organization must protect consumer data from unlawful access and release (NIST-28, 2024). PD 1 and 2 stated that data breaches, regardless of scale, can result in substantial operational, financial, and reputational consequences for an organization. When a data breach occurs, the confidentiality of sensitive information may be compromised through unauthorized extraction, leakage, or exposure to individuals or entities without proper authorization, including the public (NIST-28, 2024).

Theme 4, securing financing and costs, supports the current literature. Recent cyberattacks have resulted in significant financial losses for the affected organizations. Ransomware attacks are estimated to cost approximately \$40 million, and business email scams are estimated to cost approximately \$47 million per attack; the total estimate by 2025 is expected to reach \$10.5 trillion per year (Wang et al., 2025). To prevent these attacks, it is imperative that financial investments are made to protect consumer data. Organizations in highly regulated sectors, such as finance, healthcare, and government, must account for the expenses associated with meeting compliance standards (Manolov et al., 2025). When evaluating solutions for an organization, it is important to consider the cost structure of each platform, including licensing models, subscription plans, and total cost of ownership, because these factors influence the decision-making process (Manolov

et al., 2025). Cost remains a primary consideration when selecting an appropriate platform, requiring a careful balance between functionality, scalability, security, and overall financial impact (Manolov et al., 2025). In addition to standard subscription fees, organizations should account for ancillary expenses, including data storage, network bandwidth, and comprehensive support plans (Manolov et al., 2025). Security is a crucial aspect of contemporary software development, particularly as cyber threats continue to evolve in complexity (Manolov et al., 2025). Organizations implementing cloud-based solutions are required to safeguard their repositories, automation workflows, and deployment environments from risks such as unauthorized access, data breaches, and malicious code injection (Manolov et al., 2025). Nevertheless, cost will remain a deciding factor in what can be implemented.

Theme 4, securing financing and costs, aligns with the conceptual framework in this study. Securing financing and costs align with the RAT through being used in the decision-making process for technological solutions. In the RAT, Cohen and Felson (1979) suggested that individuals make rational choices to achieve their goals by weighing the opportunities, costs, and benefits. The authors predicted that shifts in legitimate opportunities, such as technological advances, can increase the interaction between motivated offenders and suitable targets when capable guardians are lacking (Lee & Choi, 2021). Many institutions that store valuable data, including financial, educational, political, and religious organizations, may be at risk of ransomware attacks if adequate security measures are not in place (Lee & Choi, 2021). Consistent with RAT, it is hypothesized that wealthier victims, those with higher annual revenues and larger staff

sizes—are considered more attractive targets due to their increased capacity to pay substantial ransoms. Additionally, victims possessing cyber insurance may also be viewed as appealing targets because the presence of such coverage could increase the likelihood of ransom payment (Meurs et al., 2022).

Given that sophisticated criminals may bypass even the most advanced technological measures, relying exclusively on technology does not guarantee incident prevention (Lee & Choi, 2021). Furthermore, upgrading systems can be prohibitively expensive for individuals or organizations with limited budgets. Thus, allocating resources to new systems alone is unlikely to resolve these challenges (Lee & Choi, 2021). Instead, emphasis should be placed on implementing continuous and comprehensive training and educational programs (Lee & Choi, 2021).

Business Contributions and Recommendations for Professional Practice

These research project results can benefit and support IT business practices, while revealing areas for further analysis and deeper exploration, providing IT leaders with the best cybersecurity strategies to implement within their organizations. The most important point to draw from this study is the need for IT leaders to implement effective strategies to protect consumer data from malicious actors or cybercriminals. Training employees and consumers was a very effective strategy that helped organizations protect consumer data. This strategy was shown in the findings and was also supported by recent literature. Employees constitute the primary defense mechanism against cyber threats within an organization. Ongoing training and awareness programs will provide employees with the necessary information to respond to threats to consumer data. These programs will also

keep staff up to speed on the latest incidents and protocols. Useful options include developing online security courses and studying models of potential attacks.

The subsequent theme observed was the use of security tools and capabilities needed to protect data effectively without compromising user privacy or convenience. MFA is a security measure that requires users to authenticate their identities using multiple independent credentials. MFA has had a positive impact on securing personally identifiable information and other protected data by adding significant protection for IT systems, making unauthorized access more difficult, especially in hybrid environments. Today, awareness of security principles and the use of MFA have become a priority for many organizations. Implementing MFA within enterprise environments has proven effective in mitigating risks posed by compromised credentials, thereby strengthening the protection of sensitive corporate information.

Another prevalent theme that emerged from this study is the use of cyber insurance. Cyber insurance is widely used and has become increasingly valuable for organizations, especially small- to medium-sized businesses, as cybercriminals are increasingly targeting them. In response to the evolving threat landscape, cyber insurance has become an essential risk management tool for small and medium-sized enterprises. Cyber insurance can enhance SME security in two key ways. It incentivizes applicants to implement cybersecurity controls, with insurers either mandating specific measures to obtain coverage or offering reduced premiums when adequate controls are in place. This approach can strengthen the overall security posture of insured organizations. Cyber

insurance and security compliance complement each other. Cyber insurance requires that specific controls be in place to prevent cyberattacks.

The final theme in this study is the financing and cost considerations associated with implementing IT security within an organization. Allocating funds for security initiatives from the outset is critical. When designing a system, security must be considered from the outset. This is due to the increased number of security breaches over the last decade. Security breaches have resulted in significant financial losses for large organizations, with these costs continuing to increase. Early analysis of security requirements may reduce software development and maintenance expenses by 12%–21% (Khan et al., 2024). Adequate financial resources are essential for each project and tool because insufficient budgeting for security controls, training, and associated measures can present significant challenges in securing necessary funding. Due to budget constraints and the pressure to deliver software quickly within a competitive market, security considerations are sometimes deferred until later stages of development, potentially impacting the overall software quality. Executives must prioritize security alongside profits to avoid regrettable financial and reputational losses in the event of a security incident.

Implications for Social Change

Over the past 25 years, IT has had a profound influence on society, underscoring the need for robust and effective cybersecurity measures. The results of this study carry important implications for advancing positive social change in several vital areas. Cybersecurity plays a critical role in technological progress. Recent incidents underscore

the significant consequences of failing to implement reliable and effective security platforms, tools, and strategies. Safeguarding consumer information remains a primary objective. Neglecting security measures can jeopardize an organization's reputation, profitability, and long-term success, potentially resulting in substantial financial losses. As technology continues to advance, it is essential to address these considerations thoughtfully.

The advancement of AI has heightened the importance of security tool considerations. From a cybersecurity standpoint, this progression necessitates the implementation of additional safeguards and may prompt the development of new regulations, standards, and policies governing AI, cybersecurity, and technological innovation. Solutions, such as MFA, antivirus software, firewalls, encryption technologies, and audit log monitoring, are among the proven strategies for securing sensitive information. These tools play a critical role in safeguarding consumer data and mitigating potential threats.

Executives can integrate security initiatives into their corporate culture, establishing them as standard practice for new system development and implementation. Providing employees with comprehensive training on identifying potential threats can significantly enhance an organization's security posture. Similarly, ensuring consumers are informed about how to recognize risks and safeguard their information enhances their ability to avoid scams, helping to restore trust in organizations and ultimately supporting consumer retention and acquisition. Implementing this approach may foster an environment in which consumers perceive a higher degree of safety, thereby potentially

enhancing their willingness to engage in online transactions if they are confident that their information is adequately protected.

Budgeting for and securing funding for security initiatives is key to successfully implementing a security program within an organization. This will protect the organization and the consumer. Cyber insurance is an option for organizations, especially small- to medium-sized businesses that lack the necessary capital to implement a robust security system. This is also helpful to ensure that the organization complies and that security controls are correctly configured.

Recommendations for Future Study

IT leaders can leverage the findings of this study to assess and enhance current security strategies and policies designed to protect consumer data. Future researchers should address the current limitations and incorporate diverse perspectives to improve business practices further. A small sample size, dependence on self-reported information, and potential discrepancies between verbal accounts and actual behaviors notably constrained this study. These factors may influence the applicability and comprehensiveness of the results. Subsequent research should expand its scope to mitigate these limitations and provide more inclusive insights. Integrating both quantitative and qualitative data could enhance the validity of the findings, potentially involving an analysis of security metrics, an assessment of their effectiveness, and a quantification of incidents such as data breaches or cyberattacks that have occurred in recent years.

Follow-up studies may be necessary to evaluate the long-term effects of security strategies. Future research should investigate technological advancements and their associated vulnerabilities to enhance system and network security. AI is expected to play a significant role in this regard. ITL 5 noted, “you’re going to need AI to beat AI...because you're talking about a technology that never has to sleep.” This highlights the importance of AI in today’s technology landscape. Additionally, further research on securing mobile devices and the IoT would benefit the industry by addressing current study limitations and improving organizational cybersecurity practices.

Addressing these areas allows researchers to gain a more detailed and thorough understanding of IT security strategies. As technology progresses, so do the methods used to secure information and prevent security breaches and cyberattacks. The topics covered in this study are current and will become increasingly relevant as technology continues to advance. Continued research into practical strategies for preventing security breaches and addressing concerns related to AI will be crucial to protecting consumer data as technology continues to evolve.

Conclusion

In conclusion, cybersecurity remains a critical component of the IT sector, with its importance expected to continue growing. In this qualitative pragmatic inquiry, I explored strategies IT leaders used to protect consumer data from security breaches. The study involved semistructured interviews with eight experienced IT executives. Data collection also included two publicly available industry documents that were obtained online. Using thematic analysis, four major themes were identified: employee training

and consumer awareness, development of security tools and capabilities, cyber insurance and security compliance, and securing financing and costs. These themes aligned with the conceptual framework of the RAT. This study advances the understanding of what is needed to protect consumer data from data breaches and underscores the importance of continued investigation regarding the best security tools and systems to implement as technology continues to advance. The lessons learned will contribute to the ongoing dialogue surrounding IT security and the prevention of security breaches. Technology continues to be consumed because it makes things easier or quicker; however, this convenience comes at a risk. IT leaders must plan and implement effective strategies that companies can use to protect consumer data.

Future research can provide organizations with the essential knowledge required to formulate more effective security strategies by offering a more universal and comprehensive understanding. This will enable organizations to address and resolve the challenges they encounter in preventing security breaches, particularly as technology continues to advance. Ultimately, this contributes to organizational success and stability within the rapidly evolving technology sector. It is crucial to investigate the extent to which organizations prioritize security from the outset (i.e., prevention) or address it in response to a cyber incident (i.e., reaction). Additionally, executive sponsorship and organizational culture will significantly influence the protection of consumer data within an organization. The findings of this study serve as a potent reminder that safeguarding technology requires training, continued advancements, compliance with security

standards, and capital. As AI becomes more prevalent in the technology sector and beyond, a deeper understanding of cybersecurity will be paramount.

References

- Abdullah, H. (2020). Proposition of a framework for consumer information privacy protection. *2020 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (IcABCD)*, 1–6.
<https://doi.org/10.1109/icABCD49160.2020.9183822>
- Acronis (2025). *Acronis data privacy survey reveals 64% of global consumers cite data breaches as top privacy concern. Software, digital, AI & IT industry snapshot.*
<https://www.acronis.com/en-us/pr/2025/acronis-data-privacy-survey-reveals-64-of-global-consumers-cite-data-breaches-as-top-privacy-concern/>
- Adriko, R., & Nurse, J.R.C. (2024). Cybersecurity, cyber insurance and small-to-medium-sized enterprises: a systematic Review. *Information and Computer Security*, 32 (5): 691–710. <https://doi.org/10.1108/ICS-01-2024-0025>
- Al-Zahrani, A., & Al-Hebbi, M. (2022). Big data, major security issues: Challenges and defense strategies. *Technical Journal / Tehnicki Glasnik*, 16(2), 197–204.
<https://doi.org/10.31803/tg-20220124135330>
- Ambrož, M. (2024). Pragmatic view of research of organisations. *Izzivi Prihodnosti*, 9(3), 122–149. <https://doi.org/10.37886/ip.2024.007>
- Arenas, Á., Ray, G., Hidalgo, A., & Urueña, A. (2024). How to keep your information secure? Toward a better understanding of users security behavior. *Technological Forecasting & Social Change*, 198.
<https://doi.org/10.1016/j.techfore.2023.123028>

- Balakrishnan, N., Rajendran, A., Pelusi, D., & Ponnusamy, V. (2021). Deep Belief Network enhanced intrusion detection system to prevent security breach in the Internet of Things. *Internet of Things, 14*.
<https://doi.org/10.1016/j.iot.2019.100112>
- Bentahar, A., Meraoumia, A., Bradji, L., & Bendjenna, H. (2022). Sensing as a service in Internet of Things: Efficient authentication and key agreement scheme. *Journal of King Saud University - Computer and Information Sciences, 34*(8), 5493–5509.
<https://doi.org/10.1016/j.jksuci.2021.06.007>
- Benzecry, C. E., Krause, M., & Reed, I. A. (Eds.). (2017). *Social theory now*. University of Chicago Press.
<https://press.uchicago.edu/ucp/books/book/chicago/S/bo26383995.html>
- Boss, S. R., Gray, J., & Janvrin, D. J. (2024). Be an expert: A critical thinking approach to responding to high-profile cybersecurity breaches. *Issues in Accounting Education, 39*(1), 93–121. <https://doi.org/10.2308/ISSUES-2021-094>
- Brosnan, S., Bourke, J., & Jordan, D. (2024). The systematic effects of the research impact agenda: Qualitative evidence from the Irish research sector. *Economic & Social Review, 55*(4), 593–616.
<https://research.ebsco.com/linkprocessor/plink?id=1e1a6dfa-7c0b-3665-9f18-292663cb7562>
- Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Bywaters, D., Young, S., & Walker, K. (2020). Purposive sampling: Complex or simple? Research case

examples. *Journal of Research in Nursing*, 25(8), 652-661–661.

<https://doi.org/10.1177/1744987120927206>

Chin, W. Y., & Chua, H. N. (2021). Using the theory of interpersonal behavior to predict information security policy compliance. *2021 Eighth International Conference on EDemocracy & EGovernment (ICEDEG)*, 80–87.

<https://doi.org/10.1109/ICEDEG52154.2021.9530849>

Christou, P. A. (2025). Looking beyond numbers in qualitative research: From data saturation to data analysis. *Qualitative Report*, 30(1), 3088-3100–3100.

<https://doi.org/10.46743/2160-3715/2025.7560>

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

<https://doi.org/10.2307/2094589>

Crowe, M., & Manuel, J. (2025). Qualitative research Part 2: Conducting qualitative research. *Journal of Psychiatric and Mental Health Nursing*, 32(1), 256-258–258.

<https://doi.org/10.1111/jpm.13123>

Dawadi, S. (2020). Thematic analysis approach: A step by step guide for ELT research practitioners. *Online Submission*, 25(1–2), 62–71.

<https://research.ebsco.com/linkprocessor/plink?id=6b6893a2-66a3-38ba-9919-1731f90fd2e1>

DeLiema, M., Robb, C. A., & Wendel, S. (2025). What does trust have to do with it? Training consumers to detect digital imposter scams. *Journal of Financial Crime*, 32(1), 77–97. <https://doi.org/10.1108/JFC-12-2023-0314>

Dhabliya, D., Rizvi, N., Dhablia, A., Sridhar, A. P., Kale, S. D., & Padhi, D. (2024).

Securing machine learning ecosystems: Strategies for building resilient systems.

E3S Web of Conferences, 491, 02033.

<https://doi.org/10.1051/e3sconf/202449102033>

Elhami, A., & Khoshnevisan, B. (2022). Conducting an interview in qualitative research:

The modus operandi. *MEXTESOL Journal*, 46(1).

[https://research.ebsco.com/linkprocessor/plink?id=becd1e9a-d7be-3108-8943-](https://research.ebsco.com/linkprocessor/plink?id=becd1e9a-d7be-3108-8943-22587b50860a)

[22587b50860a](https://research.ebsco.com/linkprocessor/plink?id=becd1e9a-d7be-3108-8943-22587b50860a)

Federal Trade Commission. (2021, October 27). *FTC strengthens security safeguards for*

consumer financial information following widespread data breaches [Press

release]. [https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-](https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial-information-following-widespread-data)

[strengthens-security-safeguards-consumer-financial-information-following-](https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial-information-following-widespread-data)

[widespread-data](https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial-information-following-widespread-data)

Govindan, S. K., Vijayaraghavan, H., Sahayaraj, K. K. A., & Kinol, A. M. J. (2024).

Optimizing internet-wide port scanning for IoT security and network resilience: A

reinforcement learning-based approach in WLANs with IEEE 802.11ah. *Fiber &*

Integrated Optics, 43(1), 14–42. <https://doi.org/10.1080/01468030.2024.2342275>

Guerra, C., & Ingram, J. R. (2022). Assessing the relationship between lifestyle routine

activities theory and online victimization using panel data. *Deviant Behavior*,

43(1), 44–60. <https://doi.org/10.1080/01639625.2020.1774707>

Harerimana, A., Wicking, K., Biedermann, N., & Yates, K. (2024). Preparing for data collection: The mock interview as a researcher's training tool. *Educational Research*, 66(1), 68–85. <https://doi.org/10.1080/00131881.2024.2302156>

Hartmann, T., olde Scholtenhuis, L., Zerjav, V., & Champlin, C. (2015). Mindfully implementing simulation tools for supporting pragmatic design inquiries. *Engineering Project Organization Journal*, 5(1), 4–13. <https://doi.org/10.1080/21573727.2014.981808>

Huang, L., & Cornell, K. A. (2025). From payer to protector: The evolving role of cyber insurance in ransomware defense. *2025 Systems and Information Engineering Design Symposium (SIEDS)*, 506–511. <https://doi.org/10.1109/SIEDS65500.2025.11021152>

James, L. (2023). Releases data security guide to help businesses better protect consumers' personal information. *Journal of Internet Law*, 26(9), 3–12. <https://research.ebsco.com/linkprocessor/plink?id=fb46f4fe-28f2-3990-adce-46e4171a2cab>

Joshi, C., Slapničar, S., Yang, J., & Ko, R. K. L. (2025). Contrasting the optimal resource allocation to cybersecurity controls and cyber insurance using prospect theory versus expected utility theory. *Computers & Security*, 154. <https://doi.org/10.1016/j.cose.2025.104450>

Kawar, L. N., Dunbar, G. B., Aquino-Maneja, E. M., Flores, S. L., Rondez Squier, V., & Failla, K. R. (2024). Quantitative, qualitative, mixed methods, and triangulation

research simplified. *Journal of Continuing Education in Nursing*, 55(7), 338-344–344. <https://doi.org/10.3928/00220124-20240328-03>

Kempton, N. (2023). Data breaches: Are chief information security officers now in legal peril? *The Journal of High Technology Law*, 24(2), 893.

<https://research.ebsco.com/linkprocessor/plink?id=9bf05e95-97d3-3f57-88ed-495225207a83>

Khan, R. A., Akbar, M. A., Rafi, S., Almagrabi, A. O., & Alzahrani, M. (2024).

Evaluation of requirement engineering best practices for secure software development in GSD: An ISM analysis. *Journal of Software: Evolution & Process*, 36(5), 1–19. <https://doi.org/10.1002/smr.2594>

Kullman, S. M., & Chudyk, A. M. (2025). Participatory member checking: A novel approach for engaging participants in co-creating qualitative findings.

International Journal of Qualitative Methods, 1–14.

<https://doi.org/10.1177/16094069251321211>

Leong, S. Y., & Said, H. (2024). Development and refinement of the interview protocol:

Interview questions for international school teacher retention. *International Journal of Evaluation and Research in Education*, 13(5), 3017–3027.

<https://doi.org/10.11591/ijere.v13i5.29079>

Langan, K. A. (2021). The Library Language Game: Information Literacy through the

Lens of Wittgenstein's Language Games. *Communications in Information Literacy*, 15(1). <https://doi.org/10.15760/comminfolit.2021.15.1.6>

- Lee, H., & Choi, K.-S. (2021). Interrelationship between bitcoin, ransomware, and terrorist activities: Criminal opportunity assessment via cyber-routine activities theoretical framework. *Victims & Offenders, 16*(3), 363–384.
<https://doi.org/10.1080/15564886.2020.1835764>
- Lee, Y. Y., Gan, C. L., & Liew, T. W. (2022). Phishing victimization among Malaysian young adults: Cyber routine activities theory and attitude in information sharing online. *The Journal of Adult Protection, 24*(3/4), 179–194.
<https://doi.org/10.1108/JAP-06-2022-0011>
- Li, H., Kettinger, W. J., & Yoo, S. (2024). Dark clouds on the horizon? Effects of cloud storage on security breaches. *Journal of Management Information Systems, 41*(1), 206–235. <https://doi.org/10.1080/07421222.2023.2301177>
- Maloku, A., Maliqi, R., & Gabela, O. (2024). Application of the theory of routine activities in criminology to the general crime situation in Bosnia and Herzegovina. *Pakistan Journal of Criminology, 16*(2), 669–688.
<https://doi.org/10.62271/pjc.16.2.669.686>
- Manolov, V., Gotseva, D., & Hinov, N. (2025). Practical comparison between the CI/CD platforms Azure DevOps and GitHub. *Future Internet, 17*(4), 153.
<https://doi.org/10.3390/fi17040153>
- Martin, B. A. (2020). The unregulated underground market for your data: Providing adequate protections for consumer privacy in the modern era. *Iowa Law Review, 105*(2), 865–900. <https://research.ebsco.com/linkprocessor/plink?id=d1589d5b-b8de-3c2d-a801-007fdbaf343c>

- Meurs, T., Junger, M., Tews, E., & Abhishta, A. (2022). Ransomware: How attacker's effort, victim characteristics and context influence ransom requested, payment and financial loss. *2022 APWG Symposium on Electronic Crime Research (ECrime)*, 1–13. <https://doi.org/10.1109/eCrime57793.2022.10142138>
- Muhasin, H. J., Gheni, A. Y., & Yousif, H. A. (2024). Security and information technology for big data. *Wasit Journal for Pure Sciences*, 3(2). <https://doi.org/10.31185/wjps.418>
- Mustapha, I., Vaicondam, Y., Jahanzeb, A., Usmanovich, B. A., & Yusof, S. H. B. (2023). Cybersecurity challenges and solutions in the fintech mobile app ecosystem. *International Journal of Interactive Mobile Technologies*, 17(22), 100–116. <https://doi.org/10.3991/ijim.v17i22.45261>
- Nejjari, N., Zkik, K., Hammouchi, H., Ghogho, M., & Benbrahim, H. (2024). Assessing Data breach factors through modern crime theory: A structural equation modeling approach. *IEEE Access*, 12, 92198–92214. <https://doi.org/10.1109/ACCESS.2024.3423651>
- National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1979). *The Belmont Report: Ethical principles and guidelines for the protection of human subjects of research*. U.S. Department of Health and Human Services. <https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html>

National Institute of Standards and Technology. (February 2024). *Data confidentiality:*

Detect, respond to, and recover from data breaches.

<https://doi.org/10.6028/NIST.SP.1800-29>

Novosel, L. M. (2024). Understanding the evidence: Reliability. *Urologic Nursing*, 44(3),

137-139. <https://doi.org/10.7257/2168-4626.2024.44.3.137>

Panda, V., Mishra, A., & Sharma, M. (2023). Understanding the ripple effect: Exploring

the influence of cyber crime on social media and its consumer behavior. 2023

International Conference on Sustainable Emerging Innovations in Engineering and Technology (ICSEIET), 332–336.

<https://doi.org/10.1109/ICSEIET58677.2023.10303311>

Perkins, R. C., Howell, C. J., Dodge, C. E., Burruss, G. W., & Maimon, D. (2022).

Malicious spam distribution: A routine activities approach. *Deviant Behavior*,

43(2), 196–212. <https://doi.org/10.1080/01639625.2020.1794269>

Piasecki, S., Urquhart, L., & McAuley, P. D. (2021). Defence against the dark artefacts:

Smart home cybercrimes and cybersecurity standards. *Computer Law & Security*

Review, 42. <https://doi.org/10.1016/j.clsr.2021.105542>

Pinninti, L. R. (2024). The Impact of Peer-Collaborative Strategic Reading and

Reflective Journal Writing on Orchestrated Reading Strategy Use and

Comprehension. *TESL-EJ*, 27(4). <https://doi.org/10.55593/ej.27108a3>

Prastyanti, R. A., Rahayu, I., Yafi, E., Wardiono, K., & Budiono, A. (2021). Law and

personal data: Offering strategies for consumer protection in new normal situation

in Indonesia. *Jurnal Jurisprudence*, 11(1), 82–99.

<https://doi.org/10.23917/jurisprudence.v11i1.14756>

PR Newswire. (2021, September 28). *Securing customer data tops IT leaders' priorities in 2021: Egnyte's annual data governance trends report*. PR Newswire US.

<https://research.ebsco.com/linkprocessor/plink?id=8573adfd-c8dd-35e2-8562-6261438a85e1>

Puente, S. M., & Hernández, I. N. R. (2022). Cyber victimization within the routine activity theory framework in the digital age. *Psicología*, 40(1), 265–291.

<https://doi.org/10.18800/psico.202201.009>

Quartiroli, A., Knight, S. M., Etzel, E. F., & Monaghan, M. (2017). Using Skype to facilitate team-based qualitative research, including the process of data analysis. *International Journal of Social Research Methodology: Theory & Practice*, 20, 659–666. <https://doi.org/10.1080/13645579.2016.1275371>

Ransom, K. J., Perfors, A., Hayes, B. K., & Connor Desai, S. (2023). What do our sampling assumptions affect: How we encode data or how we reason from it? *Journal of Experimental Psychology: Learning, Memory, and Cognition*, 49(9), 1419–1438. <https://doi.org/10.1037/xlm0001149>

Rietdijk, W. J. R., & Dräger, S. (2024). What every intensivist should know about: The value of limitations in clinical research. *Journal of Critical Care*, 83.

<https://doi.org/10.1016/j.jcrc.2023.154457>

Sakhare, N. N., Kulkarni, R., Rizvi, N., Raich, D., Dhablia, A., & Bendale, S. P. (2023). A decentralized approach to threat intelligence using federated learning in

privacy-preserving cybersecurity. *Journal of Electrical Systems*, 19(3), 106–125.

<https://doi.org/10.52783/jes.658>

Shah, J. K., Sharma, R., Misra, A., Sharma, M., & Joshi, S. (2023). Blockchain-enabled communication network transforms information technologies: A thematic analysis. *2023 International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT)*, 1286–1291.

<https://doi.org/10.1109/ICAICCIT60255.2023.10465876>

Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, 124.

<https://doi.org/10.1016/j.cose.2022.102974>

Spolarich, A. E. (2023). Sampling methods: A guide for researchers. *Journal of Dental Hygiene*, 97(4), 73–77.

<https://research.ebsco.com/linkprocessor/plink?id=fde0cc81-95bd-3961-a888-5e8d48fde140>

Velmurugan, S., Prakash, M., Neelakandan, S., & Radhakrishnan, A. (2024). Provably secure data selective sharing scheme with cloud-based decentralized trust management systems. *Journal of Cloud Computing*, 13(1), 1–20.

<https://doi.org/10.1186/s13677-024-00634-8>

Wang, C., Zheng, D., Liu, X., Tang, W., Xu, H., & Cao, X. (2025). Towards cost optimization in security-aware service function chaining and embedding over

multi-vendor edge networks. *Computer Networks*, 257.

<https://doi.org/10.1016/j.comnet.2024.111002>

Appendix A: Interview Protocol and Interview Questions

The interview will begin with a video call to the participant on the agreed upon date and time. I will remind the participant that they are being recorded, then begin the recording. I will introduce myself and state that this interview is being conducted via video call, being recorded and that the participant has agreed to partake in the interview. I will ask each of the questions below and listen to the answer. I will also be taking notes during the interview.

1. What strategies do you use to protect customer data from security breaches?
2. What are your methods in determining the most appropriate cybersecurity strategies to mitigate threats?
3. How did you assess the effectiveness of the strategies to protect customers from security breaches?
4. What were the key barriers to implementing your successful strategies for protecting customers?
5. How did you address the key barriers to implementing your successful strategies for customers?
6. What else can you share with me regarding this topic?

Upon completion of all the questions, I will then ask the participant if there is any additional information that they would like to add or if they have any questions. Once all questions have been asked and addressed, I will end the recording. I will thank the participant for their time and advise them that they can reach out to me for any follow-on questions.

Appendix B: Interview Protocol

Action	Script
<p>Introduce the interview and set the stage—often over a meal or coffee.</p>	<p>"Hello, thank you for taking the time to participate in this research study. I appreciate the criticality you attach to the expected findings, and I hope to add to the literature that develops strategies to protect consumer data from security breaches. I have been working on a degree for a Doctor of Business Administration for the past few years. In this study, I am exploring the strategies IT leaders use to protect consumer data."</p> <p>"A few weeks ago, you agreed to sign an informed consent form. Do you have any questions for me or any matter that requires my attention? This interview is confidential, and your identity and that of your organization shall remain anonymous and represented by codes."</p> <p>"I will collect data using semi-structured interview questions. The idea is to allow you to explain any strategies, events, and memories that answer the interview questions. During your narration, I may prompt you for further explanation and details."</p> <p>"I will need to record your responses so that I do not miss anything."</p> <p>"Note that you may rescind your decision to participate in the research anytime."</p>
<p>Ask Interview Questions to get in-depth responses. Listen for nonverbal cues. Paraphrase as needed.</p>	<ol style="list-style-type: none"> 1. "What effective business strategies did you use to protect consumer data?" 2. "How did you measure the effectiveness of the strategies you used to protect consumer data?" 3. "Describe the challenges you encountered when implementing the strategies to protect consumer data?"

Action	Script
	<p>4. "How did you overcome those barriers?"</p> <p>5. Describe how internal stakeholders influenced your strategies to protect consumer data?"</p> <p>6. Describe how external stakeholders influenced your strategies to protect consumer data?"</p> <p>7. "What additional information would you like to share about your effective strategies to protect consumer data from security breaches that we have not already discussed?"</p>
<p>Schedule transcript review either by phone or email.</p>	<p>"In a few days, I will need your assistance in authenticating my understanding of your responses to the interview questions as part of the research process. You may adjust the script or add to your initial responses if needed. I will send the transcript by email, and we can discuss it by phone if you agree."</p>
<p>Introduce a member checking review and set the stage.</p>	<p>"Thank you for agreeing to meet me today to finalize what I heard from you during the interview and the meaning I have provided for each response."</p>
<p>Wrap up the interview by thanking participants.</p>	<p>"Your contribution to this doctoral research has been most impressive, and I thank you very much for helping me to achieve the doctoral degree. I hope you will find the research findings beneficial to your organization and professional development."</p>