

1-27-2026

# Digital Trust Recovery: Effective Data Breach Management Approaches

Milbert Flores Dacayana  
*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](mailto:ScholarWorks@waldenu.edu).

# Walden University

College of Management and Human Potential

This is to certify that the doctoral study by

Milbert Flores Dacayana

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. Annie Brown, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Yvonne Doll, Committee Member, Doctor of Business Administration Faculty

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

Walden University  
2026

Abstract

Digital Trust Recovery: Effective Data Breach Management Approaches

by

Milbert Flores Dacayana

MBA, Webster University, 2020

MA Management and Leadership, Webster University, 2020

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

January 2026

## Abstract

In the digital economy, organizations face an increasing number of data breaches that compromise sensitive information and erode consumer trust. Some organizational leaders are concerned about the lack of effective strategies to manage data breaches and restore stakeholder confidence, which threatens organizations' reputation and financial stability, and long-term trust in digital systems. Grounded in cybersecurity risk management theory (CRMT) and situational crisis communication theory (SCCT), the purpose of this qualitative pragmatic inquiry was to explore the strategies employed by data managers in Virginia, Maryland, and Washington, DC, to manage data breaches and rebuild consumer trust. Participants were 10 experienced data managers who successfully addressed data breaches within financial institutions. Data were collected using semistructured interviews and company documents. Through thematic analysis, five themes emerged: (a) continuous training, (b) communication and collaboration, (c) structured incident response, (d) proactive controls, and (e) leadership and trust management. Recommendations include integrating CRMT frameworks, applying SCCT-based communication strategies, combining technical and human-centered safeguards, and offering transparent remediation to rebuild trust. Implications for positive social change include the potential for financial institution leaders, data managers, and policymakers to implement transparent breach response practices, strengthen data protection controls, and promote ethical accountability, thereby improving consumer trust and contributing to safer, more resilient digital environments.

Digital Trust Recovery: Effective Data Breach Management Approaches

by

Milbert Flores Dacayana

MBA, Webster University, 2020

MA Management and Leadership, Webster University, 2020

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

January 2026

## Dedication

To my beloved wife, Jade Kaaihue Dacayana, your unwavering belief in me has been my foundation. Your love, patience, and steadfast support have given me the strength to persevere through every challenge. Your presence in my life has been a source of constant encouragement, and for that, I am profoundly grateful.

To my daughters, Athena, Gabrielle, Lauren, and Bettina, you are my greatest blessings. Your love, resilience, and faith in me remind me every day of the importance of perseverance and the unbreakable bond of family. To my cherished niece and nephew, Angela and Samuel, your joy and support have been a light on this journey.

I also dedicate this work to the memory of my late parents, Alberto and Milagros, and my beloved brother, Dean. Not a day passes without wishing you were here to witness my accomplishments and milestones. Your love, sacrifices, and values have shaped me into the person I am today. Though you are no longer physically present, your guidance and spirit continue to inspire me.

This journey would not have been possible without every one of you. For your love, belief, and unwavering support, I am eternally grateful.

## Acknowledgments

I extend my deepest gratitude to my esteemed chairs, Dr. Annie Brown and Dr. Yvonne Doll, whose invaluable guidance and unwavering support have been instrumental throughout this journey. Your mentorship has profoundly shaped my academic growth, and I am truly grateful for your commitment to my success. Your belief in my potential has been a driving force in my pursuit of excellence.

I sincerely appreciate my mentor, Dr. Yvonne Doll, whose guidance and encouragement have been a constant source of motivation and inspiration. Your leadership and dedication to academic excellence have left a lasting impact on my scholarly development. Your support has helped me navigate challenges with confidence and determination.

To my Walden professors, faculty, classmates, and colleagues, I extend my heartfelt gratitude for your guidance, professionalism, and dedication. Your insights and support have refined my knowledge, broadened my perspective, and strengthened my skills.

To my best friend, Dr. Marco Antonio Reburiano, thank you for your wisdom, camaraderie, and unwavering support. Your belief in me has been a source of strength, reminding me of the power of friendship and intellectual collaboration.

With deep appreciation, I thank each of you for shaping my journey. Your mentorship, encouragement, and support have been invaluable, and for that, I am forever grateful.

## Table of Contents

List of Tables .....	vi
List of Figures .....	vii
Section 1 Foundation of the Study.....	1
Background of the Problem .....	2
Problem and Purpose .....	3
Population and Sampling .....	4
Nature of the Study .....	5
Research Question .....	9
Interview Questions .....	9
Conceptual Framework.....	10
Operational Definitions.....	11
Assumptions, Limitations, and Delimitations.....	13
Assumptions.....	13
Limitations .....	14
Significance of the Study .....	15
Review of the Professional and Academic Literature.....	17
Literature Review Opening Narrative.....	17
Cybersecurity Risk Management Theory .....	20
Crisis Management Theory.....	22
Application to the Applied Business Problem.....	24
Data Breaches .....	26

Relevancy of the Literature.....	31
Literature Review Organization.....	33
Transition .....	38
Section 2: The Project.....	40
Purpose Statement.....	40
Role of the Researcher .....	41
Participants.....	44
Research Method and Design .....	48
Population and Sampling .....	51
Population .....	51
Sampling .....	51
Ethical Research.....	52
Data Collection Instruments .....	54
Data Organization Techniques.....	58
Data Analysis .....	60
Reliability and Validity.....	63
Reliability.....	63
Validity .....	65
Transition and Summary.....	67
Section 3 Application for Professional Practice and Implications for Social	
Change .....	69
Presentation of the Findings.....	71

Theme 1: Education and Training..... 71

Theme 2: Communication and Collaboration..... 72

Theme 3: Structured Incident Response ..... 73

Theme 4: Proactive Integration of Controls..... 74

Theme 5: Leadership and Trust Management ..... 75

Synthesis of the Findings ..... 77

Applications to Professional Practice .....79

    Education and Training as a Preventive Strategy ..... 79

    Communication and Collaboration as Operational Cornerstones..... 80

    Structured Incident Response as a Core Capability ..... 80

    Proactive Integration of Controls for Sustainable Defense..... 81

    Leadership and Trust Management as Strategic Imperatives ..... 81

    Key Insights From the Findings..... 82

Implications for Social Change.....84

    Individual Level: Protecting Privacy and Restoring Trust ..... 84

    Community Level: Building Cyber Awareness and Resilience ..... 85

    Organizational and Institutional Level: Strengthening Accountability and  
        Governance ..... 86

    Societal Level: Advancing Stability, Security, and Public Confidence..... 87

    Cultural and Ethical Dimensions: Promoting a Culture of Digital  
        Responsibility ..... 87

    Collective Impact and Positive Social Change ..... 88

Recommendations for Action .....	89
Recommendation 1: Embed Structured Risk Management Frameworks .....	89
Recommendation 2: Operationalize Transparent Crisis Communication	
Protocols .....	90
Recommendation 3: Balance Technical Safeguards with Human-Centered	
Initiatives.....	91
Recommendation 4: Adopt Consumer-Centered Remediation Measures .....	91
Recommendation 5: Institutionalize Continuous Testing and Auditing.....	92
Recommendation 6: Dissemination of Findings and Professional	
Integration.....	93
Recommendations for Further Research.....	94
Recommendation 1: Expand the Geographic Scope.....	94
Recommendation 2: Increase Sample Size and Diversity .....	95
Recommendation 3: Conduct Comparative and Quantitative Studies.....	96
Recommendation 4: Explore Consumer and Stakeholder Perspectives .....	96
Recommendation 5: Investigate the Role of Artificial Intelligence and	
Emerging Technologies .....	97
Recommendation 6: Examine Ethical and Psychological Dimensions of	
Breach Management .....	97
Recommendation 7: Address Identified Methodological Limitations.....	98
Reflections .....	98
Researcher Bias and Preconceived Ideas .....	99

Effects of the Researcher on Participants .....	100
Transformation in Thinking.....	100
Scholarly and Professional Growth .....	101
Conclusion .....	102
References.....	105
Appendix: Interview Protocol.....	128

List of Tables

Table 1. Literature Review Sources by Type and Year ..... 18

Table 2. Recurring Words and Phrases Identified Across Participant Interviews ..... 76

List of Figures

Figure 1. Conceptual Framework Underpinning the Research..... 35

## Section 1 Foundation of the Study

In the interconnected world of 2025, characterized by pervasive digitalization, the specter of data breaches loomed large, presenting formidable challenges to both businesses and consumers. Aslam et al. (2022) highlighted that these breaches involved unauthorized access to sensitive information, ranging from personal details to proprietary business data. Such incidents not only jeopardized the confidentiality and integrity of information but also undermined the fundamental trust that underpinned digital commerce (Sato et al., 2022). X. Chen et al. (2022) reported that consumers, increasingly wary of their data's vulnerability, reconsidered their interactions with digital platforms, which disrupted established business models and revenue streams.

The repercussions of data breaches extended far beyond mere inconvenience. Hoehle et al. (2022) emphasized that these incidents had a significant impact on businesses, profoundly affecting their financial health. The compromised trust resulting from data breaches led to substantial declines in consumer confidence, which in turn led to decreased customer acquisition and retention rates (X. Chen et al., 2022). Consequently, businesses experienced measurable financial impacts as consumer trust declined. The resulting loss of trust directly affected key financial indicators, reduced revenue streams, and diminished profitability (Sato et al., 2022). Sato et al. (2022) concluded that the fallout from data breaches manifested not only as a technological or operational issue but also as a critical financial concern that demanded proactive mitigation strategies.

As business leaders grappled with the aftermath of data breaches, the imperative to safeguard sensitive information became increasingly urgent. Mawel and Sambasivam (2023) noted that the evolving regulatory landscape underscored this urgency through stringent data protection laws that mandated businesses to strengthen their cybersecurity frameworks. Moreover, the reputational damage resulting from a breach endured over time, affecting brand equity and customer loyalty (Daoud & Hamdi, 2025). Thus, as businesses navigated the digital environment, they adopted proactive measures, prioritized robust cybersecurity practices, and fostered cultures of trust that resonated with consumers who remained wary of the pervasive threats posed by data breaches.

### **Background of the Problem**

In an era dominated by digitalization, Mawel and Sambasivam (2023) noted that businesses are increasingly relying on complex digital platforms for their operations and growth. The authors explained that this shift, while beneficial, significantly escalated the risks associated with data breaches, which compromised sensitive information and undermined consumer trust—a cornerstone of digital business sustainability (Kamenjarska et al., 2020). Recent studies by Liu (2025) and Kane (2023) have illuminated the severe financial repercussions that these breaches have inflicted on businesses, including the erosion of consumer confidence and a decline in revenues and long-term viability.

The persistent evolution of cyber threats highlighted a compelling need for continued examination of data management strategies that effectively adapt to and mitigate these risks. Smits et al. (2022) and Kolevski et al. (2025) indicated that although

organizations possessed considerable knowledge of data security, the rapid advancement of cyberattack methodologies consistently outpaced existing defensive measures. This discrepancy underscored the urgency for applied research that addressed not only the immediate impacts of data breaches but also strengthened preventive strategies (Mishra et al., 2022).

In this doctoral project, I explored the application of emerging technologies and strategic frameworks that enhance the resilience of digital businesses against cybersecurity vulnerabilities. By bridging the gap between conceptual research and practical application, this study provided actionable insights that enhanced the resilience of digital security infrastructures and strengthened organizational capacity to safeguard consumer trust and financial stability.

### **Problem and Purpose**

The specific business problem was that some data managers lacked effective strategies to manage data breaches and improve consumer trust in digital platforms. The purpose of this qualitative, pragmatic inquiry was to explore the strategies employed by data managers to manage data breaches and enhance consumer trust in digital platforms. The population for this project consisted of data managers in Virginia, Maryland, and the District of Columbia (DC) who implemented effective strategies to reduce the financial risks associated with data breaches.

By examining the challenges faced by data managers in these regions, I identified strategies in their current practices and explored targeted solutions to address these challenges. In this study, I analyzed the strategies that participants used to manage

cybersecurity threats. The findings reflected participants' perspectives and experiences, which revealed practical approaches such as enhanced training in cybersecurity protocols, investments in advanced threat detection technologies, and the implementation of proactive incident response plans (Humaidi & Shahrom, 2023). These findings demonstrated that developing and implementing effective strategies for managing data breaches in Virginia, Maryland, and DC remained pivotal to safeguarding both consumer trust and organizational viability in the digital landscape.

### **Population and Sampling**

The research population consisted of 10 data managers in Virginia, Maryland, and DC who managed data breach incidents across various sectors, including government, financial services, and e-commerce. The concentration of technological industries and the presence of stringent data protection regulations in these regions made data managers in Virginia, Maryland, and DC ideal for exploring effective data breach management strategies. A purposive sampling method was employed to select a sample size of 10 data managers or information officers. The approach ensured that participants provided relevant insights into the complexities and nuances of data security and consumer trust. By deliberately selecting individuals with substantial experience and expertise in data breach management, the project gathered rich, detailed information that is directly applicable to the research objectives. Additionally, the sample size of 10 struck a balance between depth and breadth, which enabled the collection of diverse perspectives. Maintaining the feasibility of conducting in-depth interviews was imperative (He et al., 2025; Weyant, 2022).

The participation criteria included individuals with at least 2 years of experience in a data management role, directly involved in data breach response and recovery, ensuring that these participants possessed the necessary expertise to contribute valuable insights. Participants worked as data managers in the specified regions and operated within the financial services sector. These criteria ensured that participants had the relevant experience and knowledge to provide meaningful contributions to the project in the cybersecurity and financial industries.

### **Nature of the Study**

In this project, I employed a qualitative methodology, which proved effective for exploring complex and context-dependent phenomena that required rich, descriptive data. Ahn et al. (2023) highlighted that the qualitative approach enabled an in-depth understanding of the nuanced strategies and perspectives that data managers used when responding to data breaches. Pratt (2025) emphasized that qualitative methods facilitated the exploration of subjective experiences and the meanings individuals attributed to those experiences, making them well-suited for examining how data managers addressed breaches while maintaining consumer trust. This methodology aligned with the project's aim of uncovering deep insights into real-world practices and challenges that professionals faced in the field.

I adopted a pragmatic inquiry design. Silas and Rajsingh (2024) and Haughton (2023) described pragmatic inquiry as a design that integrates diverse philosophical perspectives and emphasizes practical solutions to address real-world problems. Driggers and Boyles (2024) stated that pragmatic inquiry focuses on understanding human actions

and solving problems to improve conditions. Parsons et al. (2024) explained that this design allows researchers to use multiple data collection methods, which supports flexibility and adaptability. Kelly and Cordeiro (2020) asserted that pragmatic inquiry generates actionable outcomes that directly influence business practices. I conducted semistructured interviews and analyzed publicly available documents to gather comprehensive data from data managers in Virginia, Maryland, and DC. I accessed participants through professional networks, industry associations, LinkedIn invitations, and referrals from financial institutions and cybersecurity organizations to engage experienced professionals in data breach management.

In this project, I applied the cybersecurity risk management theory (CRMT), developed by Mann (2024). Situational crisis communication theory (SCCT), introduced by Coombs (2007), was also used to analyze how financial institutions managed data breaches, restored consumer trust, and maintained economic stability (Chandna & Tiwari, 2023; Qazi, 2023). CRMT provided a structured framework that helped identify and mitigate cybersecurity risks by integrating proactive security measures, ensuring regulatory compliance, and developing effective incident response strategies. SCCT complemented this framework by explaining how organizations communicate during crises, categorizing response strategies to minimize reputational damage, and rebuilding stakeholder confidence. By applying these theories, I explored how financial institutions navigated cybersecurity challenges through both risk management and crisis communication, deriving valuable insights into best practices that strengthened their financial cybersecurity resilience.

In this study, I applied CRMT and SCCT to evaluate how financial institutions mitigate data breaches, regain consumer trust, and sustain economic stability. CRMT provided a structured approach that helped identify, assess, and manage cybersecurity risks, ensuring organizations implemented effective preventive and responsive measures. SCCT defined how organizations communicated during crises, prescribed response strategies that minimized reputational harm, and rebuilt stakeholder confidence. By integrating these theories, this study established a comprehensive framework that explains how financial institutions manage cybersecurity risks and strategically communicate during crises to preserve operational resilience.

Mann (2024) developed CRMT to establish a structured framework that assessed and mitigated cybersecurity threats through risk identification, control implementation, and compliance measures. CRMT enabled organizations to design proactive security strategies that safeguarded sensitive data and financial assets. Coombs (2007) introduced SCCT as part of crisis management theory (CMT) to explain how organizations use strategic communication to manage crises. SCCT categorized crisis response strategies—such as denial, diminishment, and rebuilding—to protect reputational integrity and restore stakeholder trust. By incorporating the contributions of these theorists, this study constructed a conceptual framework that integrates risk management and crisis response within financial institutions.

Mann introduced CRMT in 2024 as a structured method for identifying, assessing, and mitigating cybersecurity threats. This theory emerged in response to the increasing complexity of cyber risks and the growing need for financial institutions to

implement robust security measures that protect sensitive data. Coombs developed SCCT in 2007 as part of CMT to provide organizations with strategic communication frameworks that managed crises, including cybersecurity incidents. The introduction of these theories highlighted the evolving landscape of digital threats and crisis communication, reinforcing their relevance in assessing how financial institutions handled data breaches and restored stakeholder confidence.

The integration of CMT and CRMT provided a dual-weighted perspective that effectively managed data breaches. Coombs (2007) discussed that CMT addressed strategies to plan for and react to sudden, high-impact, low-probability events, which aligned with the nature of data breaches and their unpredictable elements. CMT provided organizations with a structured methodology to contain damage, restore normal operations, and learn from incidents to prevent recurrence. Organizations that used CMT, according to Valencia et al. (2024), demonstrated that crisis communication strategies maintained stakeholder trust and reassured them of the company's stability during technology breaches. At both individual and organizational levels, CMT highlighted the context surrounding specific crises. Sharma et al. (2024) emphasized that CMT approached crises through an organizational process perspective, using practical tools that helped managers prevent reputational and operational losses caused by cyber events.

CMT, which originated from Mitroff and Pearson's pioneering work, was first introduced in a 1993 publication that emphasized crisis preparedness and management, serving as a cornerstone in developing strategies to mitigate crisis events. Mitroff and Pearson stressed that organizations required well-structured methods to anticipate,

respond to, and recover from high-impact crises. Their framework emphasized the importance of planning for crises in advance and learning from them afterward, both of which minimized disruptions and built organizational resilience.

### **Research Question**

What strategies do some data managers employ to manage data breaches and improve consumer trust in digital platforms?

### **Interview Questions**

1. Describe your role in managing data security and handling data breaches within your organization.
2. What specific strategies have you implemented to prevent and manage data breaches?
3. How do these strategies align with industry best practices?
4. What significant challenges have you encountered in responding to data breaches?  
How did you overcome these challenges?
5. How have the strategies you implemented to manage data breaches impacted consumer trust in your organization?
6. How does your organization adapt its data breach management strategies in response to evolving cybersecurity threats?
7. How do you see the organization evolving its strategies in the future?
8. What proactive measures do you take to prevent data breaches?
9. Please share any additional information or insights about managing data breaches and restoring consumer trust that you would like to share that we have not discussed.

## Conceptual Framework

In this qualitative study, I employed the pragmatic inquiry design using CRMT and SCCT as the conceptual framework. CRMT, developed by Mann (2024), provides a structured and proactive method for identifying, assessing, and mitigating cybersecurity threats. Mann (2024) emphasized that CRMT required organizations to identify vulnerabilities, implement layered controls, and maintain compliance to strengthen cybersecurity readiness. Valdez et al. (2024) and Sharma et al. (2024) supported this view by demonstrating that CRMT aligns technological defenses with organizational policies to reduce cyber risks and enhance institutional preparedness. These contributions established CRMT as an appropriate framework for exploring how data managers implemented preventive strategies and strengthened breach response processes within financial environments.

In this study, I also used SCCT to explain how organizations maintained stakeholder trust during and after data breaches. Contemporary studies by Chandna and Tiwari (2023) and Qazi (2023) demonstrated that SCCT-guided responses shaped consumer perceptions during crisis events. Chandna and Tiwari (2023) demonstrated that transparent communication mitigated reputational harm, while Qazi (2023) explained that SCCT-based message strategies enabled organizations to reassure stakeholders during recovery. Sharma et al. (2024) further illustrated that structured crisis communication preserved credibility and operational stability when organizations confronted technology-related disruptions. These recent studies confirmed the relevance of SCCT as a communication-focused framework for evaluating post-breach trust restoration.

The integration of CRMT and SCCT provided a cohesive conceptual structure that aligned technical risk mitigation with strategic communication. CRMT clarified how organizations assessed risks, implemented controls, and maintained cybersecurity resilience, while SCCT explained how communication strategies influenced stakeholder trust during breach response. This dual framework aligned directly with the study's purpose, which explored how data managers in Virginia, Maryland, and Washington, D.C., managed cybersecurity incidents and rebuilt consumer trust. Research by Aslam et al. (2022), X. Chen et al. (2022), and Kochetkov (2024) supported this integrated approach, demonstrating that proactive controls, structured incident response, and transparent communication collectively strengthened digital trust and improved organizational recovery following breaches. This combined framework effectively guided the exploration of strategies that data managers used to mitigate cyber risks and restore confidence in digital platforms.

### **Operational Definitions**

*Cybersecurity risk management theory* (CRMT): A structured framework organizations use to identify, assess, and mitigate cybersecurity threats through layered controls, continuous monitoring, and regulatory compliance, designed to strengthen cybersecurity resilience (Mann, 2024).

*Crisis management theory* (CMT): An approach that guides organizations in anticipating, preparing for, responding to, and recovering from crises—including data breaches—to protect operations and maintain stakeholder confidence (Rivera, 2023).

*Data breach:* An incident in which unauthorized individuals access, disclose, or remove sensitive information, resulting in compromised confidentiality, operational disruption, and diminished consumer trust (Sato et al., 2022).

*Data manager:* A professional responsible for overseeing organizational data systems, implementing security protocols, and coordinating response activities to safeguard sensitive information in the event of a breach (Humaidi & Shahrom, 2023).

*Incident response plan:* A structured organizational protocol outlining detection, containment, mitigation, and recovery actions executed during cybersecurity incidents (Rahman et al., 2024).

*Pragmatic inquiry:* A flexible research approach that prioritizes real-world problem-solving and actionable outcomes by integrating multiple data sources and methodological tools (Driggers & Boyles, 2024).

*Proactive controls:* Preventive cybersecurity measures—such as continuous monitoring, system hardening, and employee training—implemented to reduce vulnerabilities and minimize the likelihood of a breach (Valdez et al., 2024).

*Semistructured interview:* Guided conversations that utilize predetermined open-ended questions, allowing participants to elaborate on their experiences while maintaining alignment with the research purpose (Weyant, 2022).

*Situational crisis communication theory (SCCT):* A framework that guides organizations in selecting communication strategies during crises to reduce reputational damage and rebuild stakeholder trust (Chandna & Tiwari, 2023).

*Thematic analysis*: A systematic qualitative method used to identify and interpret recurring patterns across interview data, enabling researchers to generate meaningful insights (Braun & Clarke, 2021).

### **Assumptions, Limitations, and Delimitations**

I outlined both assumptions and limitations to enhance transparency and credibility in my qualitative research. I defined assumptions as foundational beliefs that I relied on, even though I could not verify them (Lopopolo et al., 2025). These assumptions shaped my research framework and influenced its design and analysis. I defined limitations as constraints or weaknesses that I could not control, which affected the scope and applicability of my findings (Rietdijk & Dräger, 2024). By defining these elements clearly, I helped readers understand the study's boundaries and identify opportunities for future research improvements.

#### **Assumptions**

I acknowledged the underlying assumptions to ensure clarity and validity in the findings of my study (Wellberg & Evans, 2022). Previous studies, such as those by Algarni et al. (2021), who assessed cybersecurity risks quantitatively, and Shah et al. (2025), who examined the security and confidentiality of network communication, provided essential context and reinforced the importance of critically examining assumptions within the research framework. I assumed that the cybersecurity landscape, including threat vectors, security technologies, and organizational practices, remained relatively stable during my research period. However, I recognized that cybersecurity evolved rapidly as new threats and technologies emerged. I assumed that the reported

instances of data breaches were accurate and comprehensive. However, I diversified my data sources and considered the potential for underreporting or misreporting in my analysis and conclusions. I assumed that findings regarding data breach strategies and impacts were generalized across different sectors and reflected common themes and best practices that organizations could implement universally. I also assumed that organizations responded to data breaches in relatively uniform ways based on best practices and regulatory requirements. I assumed that participants provided honest and accurate responses. I further assumed that the chosen conceptual frameworks, CMT and CRMT, were applicable and relevant to the context of data breaches (Akkus et al., 2020). Finally, I assumed that all data used in the study complied with privacy laws and ethical standards.

### **Limitations**

I enhanced my understanding of the context of my study and strengthened its credibility by acknowledging its limitations (Jeremy & Spandagou, 2025). Recognizing these limitations demonstrated that I critically evaluated my work and remained aware of its boundaries, which strengthened the validity and reliability of my research. This acknowledgment clarified where my findings were most robust and where readers needed to interpret them with caution (Calini & Iossa et al., 2024). I acknowledged that I only accessed publicly reported data breaches, which limited the comprehensiveness of my findings. I recognized that cybersecurity evolved quickly, with new threats and protective technologies constantly emerging, which made my results potentially time-sensitive (Iglesias et al., 2023). I acknowledged that if my sample lacked diversity or represented

only certain types of organizations, my findings might have limited generalizability. I recognized that qualitative data interpretation carries inherent subjectivity, as researchers might interpret the same interview data differently, which could lead to varying conclusions and potential bias (Tewolde, 2023). Finally, I acknowledged that my findings depended on the honesty and accuracy of participant responses. Factors such as misremembering events, misunderstanding questions, or presenting oneself in a positive light could have introduced inaccuracies that affected the reliability of my study's conclusions (Tewolde, 2023).

### **Significance of the Study**

This study held significance for business leaders because its findings provided evidence-based strategies that strengthened cybersecurity resilience, improved breach response, and restored digital trust. Researchers such as Pang and Vance (2025) have demonstrated that organizations continue to incur substantial financial and operational losses following data breaches, underscoring the need for enhanced cybersecurity practices that mitigate these risks. Bana et al. (2025) demonstrated that breaches generated direct and indirect costs, straining institutional resources, and indicated that financial institutions would benefit from adopting more proactive and structured approaches to cybersecurity. By examining how data managers addressed breaches in real environments, this study offered insights that informed business leaders on how to reduce financial exposure, enhance operational continuity, and protect their digital ecosystems.

This study may contribute to the improvement of business practice by identifying practical methods that data managers can use to strengthen risk management, enhance

organizational communication, and streamline incident response. Janvrin and Wang (2022) emphasized that integrating cybersecurity practices into broader business continuity frameworks improved institutional decision-making and operational resilience. Sorn et al. (2024) demonstrated that organizations that understood breach mechanisms created more effective security strategies, which in turn reduced vulnerabilities. The participants' experiences in this study confirmed these findings by demonstrating that proactive education, structured incident response systems, and cross-departmental collaboration enhanced the efficiency and effectiveness of breach management. These results provided practitioners with actionable guidance that advanced business practices by aligning cybersecurity decision-making with operational priorities and organizational goals.

This study also may contribute to positive social change by identifying approaches that protected consumers, strengthened digital trust, and supported more secure digital environments. Valdez et al. (2024) explained that organizations required precise and actionable cybersecurity knowledge to sustain strong defenses, which directly influenced consumer protection and community-level trust. Aslam et al. (2022) and X. Chen et al. (2022) highlighted that improved cybersecurity practices can reduce the societal harm caused by data breaches, including privacy violations and financial losses. By presenting strategies that enhanced cybersecurity readiness and transparent communication, this study supported social well-being by helping institutions adopt practices that reduced the frequency and severity of breaches. The findings empowered

organizations to safeguard individual rights, protect sensitive information, and contribute to safer digital communities. Review of Professional and Academic Literature

### **Review of the Professional and Academic Literature**

In this section, I review professional and academic literature relevant to the research topic. I critically analyzed and synthesized peer-reviewed journal articles, government reports, and scholarly books to demonstrate the depth and scope of this inquiry. In the literature review, I identified trends and key insights related to managing data breaches and their impact on businesses. I organized the literature review to guide readers through key concepts and theories, providing a clear and concise overview of the material. To maintain academic rigor, I ensured that at least 85% of the references came from peer-reviewed sources, with the majority published within the past 5 years to reflect current knowledge and developments in the field.

#### **Literature Review Opening Narrative**

In this literature review, I examined two conceptual frameworks relevant to cybersecurity risk management within financial institutions: CRMT and CMT. These two theories underpinned the project's exploration of data breaches, offering a comprehensive understanding of how organizations effectively manage and mitigate the risks associated with cybersecurity threats. I applied these conceptual frameworks to guide the research because they provided structured approaches for understanding and addressing complex cybersecurity phenomena (Moernaut, 2021).

Within the context of cybersecurity, CMT helped organizations systematically identify, assess, and manage risks, as well as respond to and recover from incidents. The

CRMT offered a foundation for developing strategies that enabled organizations to prevent cybersecurity breaches and ensure swift recovery with minimal operational and financial damage when breaches occurred.

I critically examined literature aligned with CMT (Coombs, 2007) and CRMT (Ampel et al., 2024) to provide a clear understanding of the strategies necessary for restoring trust after a data breach. The literature I reviewed included peer-reviewed scholarly articles, academic journals, and books, with more than 85% of the sources published between 2020 and 2024. This approach ensured that the study remained relevant to the contemporary challenges of data breach management. Table 1 presents a breakdown of the references that I used in this literature review.

**Table 1**

*Literature Review Sources by Type and Year*

Source type	Published 2020–2024	Published before 2020	Total no.	% of total sources
Peer-reviewed journal article	32	12	44	67.75
Book	5	3	8	12.50
Other resource	8	4	12	18.75
Total	45	19	64	100

The purpose of this literature review is to examine research on the strategies employed by organizations—particularly financial institutions and digital platforms—to manage data breaches and restore consumer trust. The review provides a contextual understanding of how data breach incidents affected businesses and the critical frameworks that organizations used to mitigate these effects (Khan et al., 2022). I

organized the literature into four key areas: (a) cybersecurity management in preventing breaches, (b) the impact of data breaches on consumer trust and business profitability, (c) crisis management and risk management frameworks, and (d) strategies for restoring consumer trust after a breach. I compiled this literature review by conducting targeted searches for peer-reviewed sources published between 2020 and 2024. Databases such as Google Scholar, the Walden University Library, and EBSCOhost provided access to the most relevant and up-to-date research. I used keywords such as *data breaches*, *cybersecurity management*, *consumer trust*, *digital platforms*, and *financial institutions* to identify relevant studies.

In the digital age, organizations worldwide prioritize data security as a response to the growing threats of cyberattacks, data breaches, and increasing regulatory pressures. Huaman et al. (2022) explained that conceptual frameworks guiding data security provide systematic approaches for identifying and mitigating risks by defining underlying principles. These principles served as foundational building blocks of effective data security practices (Aslam et al., 2022; Alhashmi et al., 2021). Smith et al. (2020) emphasized the importance of strong encryption and multi-factor authentication in health care environments, while Franke et al. (2024) demonstrated how organizations protected sensitive financial data through blockchain technologies. These studies demonstrate that compliance with regulatory frameworks, such as the cybersecurity risk management framework (RMF), empowers business leaders to develop comprehensive policies supported by advanced technologies, thereby safeguarding information while maintaining compliance with relevant regulations. By adhering to such frameworks, organizations

strengthened their defenses against evolving cyber threats and reinforced stakeholder trust in an increasingly digital economy.

Data managers effectively address evolving cybersecurity challenges by integrating advanced technological solutions with conceptual frameworks that maintained the fundamentals of strong data security. Zhu and Wang (2025) emphasized the need to protect data integrity in e-commerce and cloud computing environments, which remained vulnerable to data tampering and unauthorized access. De Lima et al. (2025) identified the vulnerabilities inherent in distributed cloud networks and explained how these risks required continuous monitoring and mitigation. Ashtiani et al. (2025) noted that the use of hash functions, digital signatures, homomorphic encryption, and secure multi-party computation played a critical role in countering such risks.

By incorporating these theoretical perspectives, financial institutions effectively aligned their cybersecurity strategies with their business objectives. Through risk management and crisis response, these institutions preserved the quality of their operations, protected stakeholders, and enhanced the overall stability of the digital financial system. This comprehensive approach to cybersecurity demonstrated the value of conceptual frameworks in addressing the complex challenges posed by modern cyber threats.

### **Cybersecurity Risk Management Theory**

In an era of heightened dependence on information systems, financial institution managers faced immense pressure to protect data and prevent breaches. This study

applied CRMT as a macro framework to illustrate that financial institutions required a cybersecurity maturity model capable of addressing and mitigating cyberattacks (Mann, 2024). Valdez et al. (2024) and Sharma et al. (2024) emphasized the importance of CRMT in aligning technological solutions with organizational policies and preemptive strategies to prevent digital threats. The theory's core principles—risk identification, risk mitigation, and committee oversight—formed the foundation for its application. J. Z. Zhang et al. (2024) asserted that effective risk identification requires a comprehensive understanding of potential cybersecurity threats, enabling organizations to develop proactive preventive measures. Kochetkov (2024) detailed risk mitigation strategies that reduced the likelihood and impact of cyber incidents, thereby strengthening the security of operational processes.

CRMT provided a holistic framework that helped organizations understand and manage cyber threats, which was particularly critical for protecting financial institutions from digital attacks. Ampel et al. (2024) and Jarjoui and Murimi (2021) observed that CRMT established a systematic process for identifying, assessing, and managing risks that could compromise sensitive financial data. As cyberattacks increasingly targeted financial institutions due to their responsibility for safeguarding confidential information, the need for CRMT became more urgent. CRMT offered a structured classification of information and a systematic approach that enabled financial institutions to identify vulnerabilities, strengthen their defenses, and maintain readiness against evolving threats.

## **Crisis Management Theory**

Mitroff (1988) developed CMT, emphasizing that proactive preparedness mitigates the consequences of crises and enhances organizational resilience. CMT emphasized the importance of anticipating potential crises and maintaining well-developed plans to address them (Antonetti & Baghi, 2024). Proactive organizations recognized vulnerabilities and designed interventions that prevented crises from occurring. Financial organizations mitigated risks before they materialized by adopting proactive preparedness rather than reactive measures, ensuring that their responses to crises remained timely and effective. Regular security audits identified potential threats; employee training increased awareness of preventive and mitigation measures; and incident response teams provided immediate action once incidents occurred. Proactive preparedness measures enhanced organizational resilience by protecting assets, ensuring operational continuity, and safeguarding reputations. Thus, CMT defined proactive preparedness as a valuable organizational tool for preventing and managing crises. Organizations that addressed vulnerabilities proactively maintained operational stability amid widespread uncertainty and risk.

In the cybersecurity domain, structured crisis management plans with clearly defined responsibilities established organized systems that facilitated effective communication with stakeholders, enabling prompt containment of affected environments and minimizing losses. Ensuring business continuity during disruptions strengthened stakeholder confidence and organizational resilience. CMT, when supported by a structured response plan, proved essential for reducing the impact of crises and

maintaining operational continuity through clarity, preparedness, and rapid action. CMT also emphasized the recovery process, which remained vital for restoring normal operations and rebuilding trust after crises (Rivera, 2023). Effective recovery strategies included data restoration, system repairs, and coordinated public relations efforts to communicate with stakeholders and manage reputational damage (Fang et al., 2023). After cybersecurity incidents, organizations not only addressed technical vulnerabilities but also reassured customers and partners about the safety of their data (Pang & Vance, 2025). Well-structured recovery plans enabled organizations to resume operations quickly and reduce the long-term effects of crises.

Coombs (2007) further advanced CMT as a structured framework for analyzing and addressing organizational crises, including data breaches. Coombs (2007) argued that organizations need to respond strategically to crises in order to mitigate damage and restore trust. Within the context of data breaches, CMT provided valuable insights into how organizations manage post-breach recovery, communicate effectively with stakeholders, and restore consumer confidence (Sharma et al., 2024). Coombs (2007) outlined three key phases of crisis management—pre-crisis, crisis response, and post-crisis—each requiring targeted strategies to minimize the impact of data breaches and rebuild trust. Rivera (2023) explained that CMT guided organizations in managing not only technical challenges but also reputational and trust-related repercussions. Al (2020) noted that CMT underscored the importance of proactive measures such as maintaining a well-defined incident response plan and engaging in transparent communication with consumers during and after a breach.

Integrating insights from CRMT and CMT provided a robust conceptual foundation for this study. By examining how financial institutions manage and mitigate cybersecurity risks, I identified effective strategies that enhance both operational and financial stability. The combined application of these two management theories supported a holistic approach to cybersecurity that encompassed technological solutions, organizational policies, and crisis management practices. Nie et al. (2020) and Ozarpa et al. (2025) indicated that insights derived from applying these two theories contributed to the broader cybersecurity discipline by revealing effective practices and highlighting areas for improvement in risk management strategies. This comprehensive integration ensured that the study addressed the multifaceted nature of cybersecurity challenges within financial institutions and demonstrated how organizations improved resilience against cyber threats.

### **Application to the Applied Business Problem**

In this qualitative pragmatic inquiry, I explored the strategies that data managers in Virginia, Maryland, and Washington, D.C., used to manage data breaches and restore consumer trust in digital platforms. Data breaches produced far-reaching repercussions for businesses, affecting both financial viability and consumer confidence for years after the incidents occurred. Morgan et al. (2021) emphasized that organizations that failed to handle data breaches effectively experienced significant declines in customer loyalty, resulting in substantial revenue losses and diminished sustainability. Deshpande and Damle (2025) found that organizations that applied transparent communication and

reinforced cybersecurity frameworks effectively mitigated adverse outcomes and restored consumer trust.

The findings revealed two critical implications: businesses needed both immediate crisis response strategies and long-term trust-building initiatives. While financial losses caused immediate harm, the erosion of consumer loyalty had lasting effects that jeopardized the organization's viability. Companies that have adopted transparency and implemented robust security measures have demonstrated accountability, regained consumer trust, and maintained a competitive edge. The study confirmed that the comprehensive impact of data breaches extended across financial, operational, and legal dimensions. Understanding these effects enabled organizations to develop more effective strategies for both preventing breaches and recovering from them when they occurred.

This study also considered the unique needs of businesses operating in Virginia, Maryland, and Washington, D.C. Coombs (2007) emphasized that organizations that prepared for crises and communicated transparently were more likely to preserve consumer trust and minimize financial damage. I incorporated the data protection priorities identified by J.J. Zhu et al. (2024), the mitigation strategies proposed by Sato et al. (2022), and the innovative applications of artificial intelligence described by Rahman et al. (2024). Integrating these insights produced a comprehensive and actionable framework that guided organizations in addressing data breaches holistically. The strategies focused on prevention, mitigation, and the restoration of consumer trust, particularly within high-risk and data-sensitive industries in the region.

## **Data Breaches**

Effective cybersecurity management has prevented data breaches, which remain critical as organizational leaders increasingly adopt interconnected environments, such as IoT-powered smart cities. Kure et al. (2022) identified an urgent need for adequate cybersecurity approaches to protect these systems from malicious attacks and unauthorized misuse. The researchers explained that IoT environments were more vulnerable to attack due to their interconnected nature, making proactive measures essential to ensuring greater security. H. Zhang et al. (2025) further demonstrated that the integration of personal and critical information within these systems heightened the risk of breaches. Researchers called for stricter security laws, evolving cybersecurity practices, and more robust frameworks to mitigate such risks. The findings from these studies strengthened the conceptual foundation of this research and ensured the practicality of the identified strategies, addressing both existing vulnerabilities and emerging threats.

Data breaches extended beyond technical vulnerabilities, inflicting financial losses and eroding consumer trust. Pang and Vance (2025) found that data breaches caused significant harm, including lost revenue and long-term reputational damage, particularly in sensitive sectors such as health care and financial services. Hoehle et al. (2022) emphasized the necessity of post-breach compensation strategies to rebuild trust and loyalty among affected customers. Malatji (2024) demonstrated that effective cybersecurity management protects data integrity and serves as a safeguard for financial stability and reputation. These findings underscore the severe repercussions of data

breaches and reinforce the need for effective cybersecurity practices. Breach response strategies that integrated proactive measures equipped organizational leaders with the tools necessary to manage both the immediate and long-term impacts of a data breach.

Because cyber threats continuously evolve, security frameworks require ongoing adaptation. Ampel et al. (2024) proposed incorporating hacker community analytics into threat intelligence to enhance resilience through real-time insights into emerging threats. Abasi-amefon et al. (2023) advocated educational initiatives, such as hackathon-based learning, to promote the development of practical cybersecurity skills. Malatji (2024) emphasized the need to secure diverse environments, including smart cities, which rely on complex infrastructures. These studies collectively demonstrated that cybersecurity required more than advanced technologies—it depended equally on human capability and collaboration. Ampel et al. (2024) confirmed that analyzing hacker community data provided organizations with strategic advantages through predictive threat intelligence. Abasi-amefon et al. (2023) further demonstrated that experiential learning activities, such as hackathons, enhance professional expertise, creativity, and innovation, enabling cybersecurity professionals to anticipate and counter sophisticated attacks effectively.

Data breaches have undermined consumer confidence, significantly affecting business profitability and long-term success. Pang and Vance (2025) found that organizations experiencing data breaches suffered substantial revenue losses and sustained damage to their customer relationships. Algarni et al. (2021) recommended compensatory strategies that aligned with consumer expectations to rebuild trust and loyalty, emphasizing a consumer-centered approach to recovery. Together, these studies

illustrated that effective breach response required organizations to address both financial and relational dimensions to achieve immediate recovery and long-term trust restoration.

Effective communication and transparency have proven essential for reporting online fraud and restoring consumer confidence following data breaches. L. Kim (2021) observed that many victims of online scams avoided reporting incidents because they distrusted existing systems and feared further victimization. L. Kim (2021) emphasized that organizations needed to foster trust-based mechanisms that encouraged reporting. Without such mechanisms, organizations risk underreporting incidents, thereby obscuring the true extent of cyber fraud and hindering the development of effective countermeasures. Similarly, J.J. Zhu et al. (2024) confirmed that transparent, timely, and honest communication was vital for rebuilding consumer confidence and ensuring long-term profitability after a breach. Openness in communication not only restored trust but also reduced reputational damage and encouraged customer loyalty. Collectively, these studies highlighted the interdependence between communication, trust, and transparency in strengthening organizational resilience against fraud and data breaches.

Business leaders strengthened cybersecurity effectiveness by combining technological advancement with an organizational mindset that prioritized consumer confidence and sustainability. Abasi-amefon et al. (2023) and Mahuwi and Israel (2024) found that transparency served as a critical component of consumer trust, demonstrating to customers that their data remained secure in an increasingly competitive digital marketplace. Schneier and Vance (2025) emphasized the technical importance of maintaining robust cybersecurity protections, including advanced threat detection

systems and timely security updates, to safeguard consumer information and maintain organizational credibility. These findings demonstrate that effective cybersecurity strategies strike a balance between technological innovation and organizational practices to enhance resilience, foster trust, and sustain financial stability in a dynamic digital economy.

Post-breach strategies, particularly compensation measures, played a vital role in rebuilding consumer trust and ensuring long-term organizational recovery. Ullah and Nabii (2022) identified compensation strategies as key mechanisms for restoring consumer confidence. Their longitudinal study of Target's 2013 data breach illustrated that well-implemented compensation initiatives positively influenced consumer perceptions of fairness and justice, mitigating damage to trust and loyalty. Compensation strategies that aligned with fairness principles reduced reputational harm and demonstrated corporate accountability. While these strategies carried potential financial costs, they provided significant long-term benefits by restoring relationships and maintaining profitability. Business leaders who prioritized these initiatives successfully rebuild trust and strengthened organizational resilience.

Data breaches represented a multifaceted threat that eroded consumer faith and undermined business performance, especially in industries where trust defined success. H. S. Chen and Jai (2021) confirmed that breaches diminished consumer confidence and loyalty, particularly in hospitality and service sectors. Cheng et al. (2024) emphasized that compensation strategies addressing fairness and justice improved post-breach recovery and consumer retention. L. Kim (2021) highlighted that transparency in

communication sustained trust and motivated consumers to report issues. These findings collectively demonstrate that business leaders must strengthen their defenses against cyberattacks while employing transparent and fair recovery approaches that prioritize the restoration of trust. By focusing on compensating affected individuals and demonstrating accountability, organizations rebuild consumer relationships and promote long-term growth in increasingly complex digital environments.

Compensatory actions remained crucial for repairing damaged customer relationships. Uddin et al. (2024) found that offering post-breach compensation, such as free credit monitoring or financial restitution, mitigated negative perceptions among consumers. Compensation aligned with fairness and justice principles signaled that organizations valued their customers and sought to make amends (Raza et al., 2023). These actions addressed both immediate harm and long-term loyalty, strengthening customer relationships and corporate reputation.

Integrating consumer feedback into the recovery process proved equally critical. Yang et al. (2024) demonstrated that feedback management significantly contributed to rebuilding trust after a breach. Organizations that actively solicited and addressed customer concerns gained insights into consumer expectations and fears. Incorporating feedback enabled organizations to tailor recovery strategies more effectively, ensuring that post-breach interventions aligned with customer needs and strengthened public trust. In this study, I examined the strategies employed by data managers in Virginia, Maryland, and Washington, D.C., to manage data breaches and restore consumer trust in digital platforms. I applied CMT and the RMF, developed by the National Institute of

Standards and Technology (NIST, 2018), to analyze how organizations navigated the complexities of digital breaches.

The reviewed literature underscored the importance of balancing technical cybersecurity measures with effective communication and compensation strategies. Sharma et al. (2024) and I. Kim et al. (2024) asserted that addressing both technical and relational aspects of cybersecurity was essential for minimizing the impact of data breaches and restoring consumer confidence. For example, technological advancements in cybersecurity have proven most effective when paired with transparent communication strategies that reassure customers and reinforce trust in the organization (Coombs, 2007; Ampel et al., 2024). This integrated approach allowed business leaders to navigate the evolving threat landscape with agility, ensuring resilience as digital risks continued to grow in complexity and frequency.

### **Relevancy of the Literature**

The reviewed literature is directly related to the applied business problem because it provides a multidimensional understanding of how organizations manage data breaches, mitigate risks, and rebuild consumer trust—objectives that guided this study. The literature demonstrates that data breaches pose severe operational, reputational, and financial risks, and that effective management requires both technological preparedness and strategic communication grounded in CRMT and CMT.

CRMT provided a structured process for identifying, assessing, and mitigating cyber risks through proactive governance, layered controls, and compliance with evolving regulatory requirements (Ampel et al., 2024; Sharma et al., 2024). These

principles reflected the experiences of data managers in Virginia, Maryland, and Washington, D.C., who emphasized preventive controls, coordinated responses, and continuous improvement as essential elements of digital resilience. Likewise, organizations applied CMT as an analytical lens to anticipate, contain, and transform crises such as data breaches into learning opportunities. Coombs (2007) and Rivera (2023) demonstrated that leaders who communicated transparently, promptly, and empathetically minimized reputational damage and preserved stakeholder confidence—findings that aligned with the practices identified in this study.

The reviewed research demonstrated that integrating CRMT and CMT generated a holistic model that aligned technological, procedural, and behavioral factors. Studies by Hoehle et al. (2022), J.J. Zhu et al. (2024), and Rahman et al. (2024) confirmed that cybersecurity effectiveness depended on both robust controls and a culture of trust and accountability. This alignment underscored the relevance of the literature to the research question by confirming that a dual emphasis on technical safeguards and communication strategies strengthened organizational capacity to manage crises effectively.

Additionally, the literature's focus on consumer trust restoration remained central to the business problem. Researchers such as Bana et al. (2025) and H. S. Chen and Jai (2021) identified trust as the decisive factor influencing post-breach recovery, consumer loyalty, and long-term profitability. Their findings validated the need to examine not only breach prevention but also post-incident remediation, a dimension that this study addressed. The reviewed studies collectively provided empirical and theoretical support

for the argument that organizations rebuilt confidence through transparency, fair compensation, and continuous education.

The reviewed literature also maintained relevance because it included recent studies published between 2020 and 2025, which ensured alignment with the rapidly evolving cybersecurity landscape. By synthesizing contemporary findings with foundational theories, the literature bridged conceptual understanding and practical application. Demonstrating ongoing relevance to modern cybersecurity practice and business sustainability, the reviewed literature established that the study's conceptual frameworks remained applicable to current organizational challenges. Consequently, the literature also informed the study's purpose—to identify effective strategies that data managers used to manage data breaches and restore consumer trust in digital platforms—thereby providing a strong scholarly foundation for the subsequent analysis.

### **Literature Review Organization**

The conceptual framework for this study was grounded in CMT and the RMF, both of which provided structured approaches for addressing and mitigating the impacts of cybersecurity incidents in financial institutions. These theories provided a framework for understanding and mitigating the complexities associated with digital breaches, thereby ensuring the stability and security of organizational operations. Formentin and Coombs (2012) developed CMT and emphasized that the theory's focus on effective communication and strategic response was essential for managing crises, including data breaches, within organizations.

The connection between cybersecurity practices and broader business continuity efforts underscored the strategic importance of this framework. Janvrin and Wang (2022) demonstrated that a well-integrated approach linked cybersecurity practices with overall risk management and business continuity strategies. This integration enabled financial institutions to treat cybersecurity incidents not as isolated events but as components of a comprehensive risk management process. By aligning cybersecurity measures with organizational objectives, institutions enhanced their ability to recover from disruptions while supporting strategic decision-making that sustained operational and financial stability. Organizational leaders have faced considerable challenges in managing data breaches that jeopardize operations, erode consumer trust, and threaten their long-term viability (Rosati et al., 2022).

Figure 1 illustrates the dynamic interplay between these frameworks, providing a holistic perspective on how financial institutions effectively manage cybersecurity risks. By aligning theoretical foundations with practical applications, this integrated approach strengthened institutional capacity to navigate an evolving threat landscape. This framework established the foundation for examining how these theories influenced organizational decision-making and resilience-building in cybersecurity management.

**Figure 1**

*Conceptual Framework Underpinning the Research*



Note. The figure was created by the author to illustrate the integration of Crisis Management Theory, Protection Motivation Theory, and Risk Management Framework concepts as applied to data breach management. The conceptual relationships are informed by Haag et al. (2021) and Janvrin and Wang (2022).

The ramifications of digital breaches on financial institutions were profound, extending from eroded customer trust to compromised financial stability (Bana et al., 2025). The direct financial implications included legal expenses, regulatory penalties, and the costs of remedial actions. Indirectly, breaches led to declines in customer loyalty, reduced business volume, and had an adverse impact on profits and revenue (Labrecque et al., 2021).

Organizations incurred substantial costs when responding to and recovering from cybersecurity incidents. These expenditures included hiring cybersecurity experts, investing in advanced security technologies, and ensuring compliance with legal and regulatory requirements. Pang and Vance (2025) and Bana et al. (2025) emphasized that indirect costs—such as operational disruptions, productivity losses, and reputational harm—intensified the financial burden. These researchers also highlighted long-term consequences, including increased insurance premiums and regulatory penalties, which strained institutional resources. Analysis of this evidence revealed that mitigating such costs required a strategic approach integrating both immediate response mechanisms and long-term resilience planning. The broader implications underscored the necessity for comprehensive risk management strategies that strengthened organizational preparedness and financial recovery.

In the rapidly evolving field of cybersecurity, understanding the mechanisms of data breaches remains essential for shaping effective security strategies (Sorn et al., 2024). Data breaches posed severe threats to both financial stability and organizational

reputation. Garg (2020) argued that organizations needed to adopt proactive and informed approaches to cybersecurity to remain resilient. As breaches occurred with increasing frequency, leaders prioritized rapid response measures and consistent security reinforcement. Valdez et al. (2024) asserted that organizations needed detailed, actionable empirical knowledge to maintain strong defenses against evolving cyberattacks. This study reinforced those insights by identifying concrete practices that strengthened cybersecurity postures and aligning practical solutions with theoretical frameworks. The results provided a comprehensive foundation for enhancing organizational cybersecurity measures.

This research on data breaches contributed to positive social change by offering actionable strategies and recommendations that strengthen security frameworks protecting individuals, institutions, and communities. Safeguarding personal and financial data proved critical to maintaining privacy and economic stability. Shah et al. (2025) and Algarni et al. (2021) emphasized that effective cybersecurity strategies preserved individual dignity and trust in digital environments. These strategies reinforced the importance of privacy as a cornerstone of public confidence, economic integrity, and organizational accountability. Ozarpa et al. (2025) and Kane (2023) further affirmed that the adoption of proactive cybersecurity practices promoted societal well-being across diverse organizational and geographic contexts.

The evidence demonstrated that cybersecurity, quality of life, and social development were closely interconnected. Kumar et al. (2025) and Algarni et al. (2021) reiterated that effective management strategies for cybersecurity risks were essential to

protecting both personal and institutional interests. Fang et al. (2023) and Kane (2023) confirmed that these protections played a critical role in fostering trust, security, and stability in digital interactions. Uddin et al. (2024) and Smith et al. (2020) demonstrated that integrating proactive measures and organizational culture enhances resilience and restores consumer trust within digital ecosystems. Abu et al. (2023) and Mora-Navarro (2022) provided further evidence that sound cybersecurity measures were not only vital for organizational success but also instrumental in advancing social development in increasingly digital societies. This integrated perspective aligned cybersecurity advancement with broader objectives of sustainability, trust, and societal progress.

### **Transition**

In Section 1, I conducted a comprehensive analysis of academic and professional literature, emphasizing how CMT and the RMF functioned as critical tools for managing data breaches and restoring consumer trust. I examined how businesses, particularly those in finance and digital sectors, integrated these frameworks to develop effective responses to digital threats. The findings demonstrated that combining technical cybersecurity advancements with transparent crisis communication was essential for rebuilding consumer confidence and sustaining long-term business performance.

In Section 2, I describe the methodological approach that guided this research. I outlined my role as the researcher, discussed ethical considerations, and explained the qualitative methodology employed in this study. I justified the selection of a pragmatic inquiry design, demonstrating its suitability for exploring the real-world complexities of data breach management. I detailed the population, sampling methods, and participant

criteria to ensure that the study captured the authentic experiences and insights of data managers who managed breaches. I also explained the data collection methods, particularly the use of semistructured interviews, and discussed strategies implemented to ensure reliability and validity. To enhance the study's trustworthiness, I employed member checking, which allowed participants to validate my interpretations of their responses.

In Section 3, I present the findings derived from the data analysis and aligned them with the overarching research question. I analyzed the key themes that emerged from participant interviews and connected them to the conceptual frameworks and existing literature on data breach management. The findings provided a nuanced understanding of the strategies data managers employed to rebuild consumer trust following breaches. Finally, I discussed the practical implications for business leaders, presented recommendations for future research, and summarized the significant findings, ensuring their relevance to both academic and applied business contexts.

## Section 2: The Project

### **Purpose Statement**

The purpose of this qualitative, pragmatic inquiry was to explore the strategies employed by data managers to manage data breaches and enhance consumer trust in digital platforms. In this section, I explained the ethical measures that guided this research project and protected participants' rights and well-being. I assumed full responsibility for collecting data ethically and adhered to the principles outlined in the *Belmont Report* (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979), which emphasizes respect for persons, beneficence, and justice. I reflected on my connection to the research topic and participants and outlined the steps I took to mitigate potential bias. I described the informed consent process to ensure that participants fully understood their involvement before agreeing to participate. To safeguard confidentiality, I securely stored all collected data for 5 years and properly disposed of it after the end of that period. I ensured full compliance with Walden University's Institutional Review Board requirements and maintained the highest ethical standards throughout the research process.

Participants retained the right to withdraw from the study at any stage without penalty. To facilitate this process, I provided clear instructions on how they could notify me of their decision via email or phone. Establishing a structured withdrawal process reinforced ethical research standards and promoted transparency. By maintaining a straightforward process, I respected participants' autonomy and fostered trust, ensuring

compliance with institutional and regulatory guidelines while protecting participants' rights.

I did not offer any incentives during the recruitment process. I encouraged participation by clearly communicating the study's purpose, relevance, and expectations. I emphasized the importance of each participant's professional experience and how their insights would strengthen the understanding of data breach management. I increased engagement by maintaining transparency, respect, and consistent communication throughout the study. These actions motivated participants to take part without relying on compensation and supported the recruitment of a committed and diverse group. I ensured that all participation remained voluntary, informed, and free from any form of financial influence.

### **Role of the Researcher**

In this qualitative pragmatic inquiry, I explored the strategies that data managers in Virginia, Maryland, and DC used to manage data breaches and restore consumer trust in digital platforms. As a researcher, I served as the primary instrument for data collection and interpretation, which is a hallmark of qualitative research. Berg et al. (2025) emphasized that researchers' direct engagement with participants fosters a deeper understanding while maintaining ethical rigor.

I respected participants' individuality, recognizing that their unique experiences enriched the quality of data collected during interviews. Charura (2020) noted that acknowledging participants' perspectives improved the accuracy and depth of qualitative data. This sensitivity was especially vital when discussing emotionally charged topics

such as data breaches. Husband (2020) emphasized that researchers must remain attentive to participants' emotional responses when addressing sensitive subjects. To accommodate these ethical considerations, I conducted semistructured interviews, allowing participants to share experiences openly while I guided the discussion toward relevant themes.

To mitigate potential bias, I employed reflexivity throughout the research process. Reflexivity required me to critically examine my own assumptions and monitor how they influenced the data collection and interpretation process. Olmos-Vega et al. (2023) emphasized that reflexivity enhances self-awareness and objectivity in qualitative research. I maintained a reflexive journal to document my thoughts, methodological decisions, and potential biases. I also engaged in peer debriefing and periodic self-assessments to ensure transparency. This reflective practice enabled me to maintain ethical integrity and provide balanced interpretations of participant data.

In this research, I adhered strictly to the principles outlined in the *Belmont Report* (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979), which include respect for persons, beneficence, and justice. These principles served as the foundation for protecting human subjects, ensuring that participants' rights, dignity, and welfare remain paramount. Respect for persons required that I obtain informed consent from all participants. I ensured that participation was voluntary and that each individual fully understood the study's purpose, methods, and potential risks. Bos and Bunnik (2022) asserted that informed consent represents not only a legal requirement but also a moral commitment that builds trust between researchers and participants. The consent process included a detailed explanation of the research

objectives, procedures, and possible risks, as emphasized by Berret and Munzner (2025). George et al. (2023) noted that providing clear, transparent information empowers participants to make voluntary and informed decisions regarding their participation.

The study also aligned with the principle of beneficence by minimizing harm and maximizing benefits for participants and society. The *Belmont Report* (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979) instructed researchers to evaluate potential risks and enhance benefits. Given the sensitive nature of this study on data breaches, I took proactive measures to safeguard the emotional well-being of participants. Morrow et al. (2023) emphasized that researchers have an ethical duty to implement measures that protect participants, particularly when dealing with sensitive topics. Resources, I provided participants with access to mental health resources should any emotional or psychological distress arise during or after their participation.

The principle of justice guided participant selection, ensuring fairness and impartiality. I followed Beauchamp and Childress's (2022) biomedical ethics framework to select participants equitably based on research relevance rather than convenience or vulnerability. Justice ensured that all participants had an equal opportunity to benefit from the study and that no group should bear a disproportionate share of risks or burdens. This approach guaranteed that the study's findings contributed equitably to advancing knowledge and improving organizational practices.

I meticulously followed the ethical guidelines established by the National Commission for the Protection of Human Subjects of Biomedical and Behavioral

Research (1979). Participants engaged voluntarily with full knowledge of the project's purpose and risks. By adhering to these ethical standards, I advanced my understanding of data breach management while safeguarding participants' rights, dignity, and well-being.

To preserve confidentiality, I implemented strict data protection protocols. I encrypted all digital records using Advanced Encryption Standard 256 technology and stored them on a secure, access-controlled cloud platform. I locked physical records in a tamper-proof, fireproof cabinet located in a secure facility. Franke et al. (2024) noted that compliance with the General Data Protection Regulation ensured global data privacy standards, while Seyed et al. (2023) confirmed that adherence to the Health Insurance Portability and Accountability Act protected sensitive U.S. data. I will retain all data for 5 years, and subsequently, I will destroy it by securely using digital data-wiping software and document shredding to prevent unauthorized access. These measures upheld participant confidentiality and ensured compliance with ethical and legal standards. I used an interview protocol to maintain consistency across all interviews, ensure that each participant received the same questions, and reduce the risk of interviewer bias. A structured protocol also helped me strengthen the credibility and dependability of the study by providing a precise sequence for questioning, prompting, and closing each interview.

### **Participants**

This qualitative pragmatic inquiry focused on 10 data managers employed in organizations within Washington, D.C., Maryland, and Virginia. These professionals

managed and responded to data breaches in sectors highly vulnerable to cybersecurity threats, such as financial services, health care, government, retail, and e-commerce.

Nikkhah and Grover (2024) noted that these industries faced heightened risk due to the sensitivity of the data they handled and the stringent regulatory requirements associated with it. Similarly, Durcikova et al. (2024) emphasized the importance of robust cybersecurity practices in such regulated environments, which made these regions and sectors particularly relevant to the project.

Participants met specific criteria in four areas:

- experience: at least 2 years of direct experience in managing data breaches or implementing cybersecurity strategies;
- geographical location: current employment within Washington, DC, Maryland; or Virginia;
- sector representation: employment in high-risk sectors such as financial services, government, health care, retail, or e-commerce; and
- role: a position as a data manager, cybersecurity lead, or equivalent role responsible for data breach management.

The estimated population size ranged from 200 to 250 professionals, based on industry reports and professional networks, which reflect the density of data-driven organizations in these regions. I recruited participants through professional networks, cybersecurity associations, and LinkedIn. I distributed formal email invitations that outlined the study's purpose, eligibility requirements, and the expected time commitment. I also networked through cybersecurity forums and regional conferences across Washington, D.C.,

Maryland, and Virginia to broaden outreach. H. S. Chen and Jai (2021) emphasized that organizations handling sensitive information were particularly vulnerable to breaches, making this population an ideal target for exploring effective data breach management strategies.

### **Research Method**

The methodology I used established a robust framework for understanding how data managers in Virginia, Maryland, and DC addressed data breaches. By adhering to strict ethical principles, employing reflexive and transparent practices, and applying rigorous qualitative methods, I generated credible and actionable findings. These results contributed to advancing cybersecurity practices and provided data managers with practical strategies to strengthen consumer confidence and organizational resilience in the digital age.

I selected a qualitative research method for this project because it effectively explores complex, real-world issues that require an in-depth understanding. Weyant (2022) highlighted that qualitative methodology enabled researchers to gather rich, detailed data that provided insight into participants' experiences and perspectives, particularly when the goal was to explore processes or strategies in their natural contexts. This method aligned with my objective of understanding how data managers in Virginia, Maryland, and DC managed data breaches and restored consumer trust in digital platforms. Since the study did not aim to test hypotheses or quantify variables, I found quantitative methodology inappropriate, as it focuses on numerical measurement and statistical validation (Maxwell, 2022). I also determined that mixed-methods research,

which combines qualitative and quantitative approaches, was unsuitable for this project because it concentrated exclusively on in-depth exploration rather than generalization through statistical analysis.

I employed a qualitative research method because it enabled me to explore the complex and context-specific strategies that data managers used when responding to data breaches. Weyant (2022) explained that qualitative research generates rich and detailed descriptions of participant experiences, making this method suitable for examining real-world cybersecurity practices. This approach aligned with the study's purpose because the research question focused on understanding how data managers managed breaches rather than measuring variables or testing hypotheses.

I selected a qualitative methodology over a quantitative one because quantitative methods rely on numerical analysis and hypothesis testing, which do not capture the depth of participants' experiences or the nuanced reasoning behind their strategies. Maxwell (2022) confirmed that qualitative research remained appropriate when researchers sought to understand meaning, processes, and lived experiences rather than statistical relationships. I also determined that mixed-methods research was unnecessary because the project's scope required concentrated exploration rather than triangulation through numerical measurement.

The qualitative method supported the study's alignment with a pragmatic inquiry design. Driggers and Boyles (2024) emphasized that pragmatic inquiry addressed real-world problems by generating practical solutions grounded in participant knowledge. This perspective reinforced the selection of qualitative methodology because it permitted

flexibility and focused on actionable insights relevant to business practice. Tingare et al. (2024) noted that pragmatic inquiry accommodates diverse data sources and emphasizes practical outcomes, thereby strengthening the suitability of qualitative methods for cybersecurity research.

I used semistructured interviews to gather firsthand accounts from data managers in Virginia, Maryland, and DC. Weyant (2022) noted that semistructured interviews encouraged open-ended responses while maintaining alignment with the research question, which enhanced the depth and quality of the data collected. These interviews enabled me to examine how participants interpreted, implemented, and refined data breach management strategies within their organizations.

I supplemented interviews with document analysis to strengthen methodological rigor. Braun and Clarke (2021) emphasized that document analysis complemented interview data by providing additional context and validation. This combination of methods supported a holistic, qualitative approach that aligned with best practices in cybersecurity research, thereby improving the trustworthiness of the findings. Therefore, the qualitative method provided a practical foundation for this study. It enabled me to capture the depth of participants' lived experiences, justify methodological decisions with contemporary scholarship, and generate practical insights for improving data breach management within financial institutions and digital organizations.

### **Research Method and Design**

I adopted a pragmatic inquiry design, which effectively addressed practical, real-world challenges by emphasizing actionable solutions. Driggers and Boyles (2024)

described pragmatic inquiry as a flexible and outcome-oriented approach that integrates diverse philosophical perspectives to solve applied problems. This design was particularly appropriate for the project because it supported the examination of how data managers manage data breaches, a pressing and complex issue in today's digital environment. Pragmatic inquiry emphasized practical application and methodological adaptability, making it an ideal approach for exploring the strategies that data managers employed to mitigate breaches and rebuild consumer trust (Tingare et al., 2024).

A pragmatic inquiry design aligned with the purpose of the study and guided the exploration of how data managers managed data breaches and restored consumer trust in digital platforms. Driggers and Boyles (2024) described pragmatic inquiry as a design that emphasized problem-solving and real-world application. Their description demonstrated that the design facilitated a clear understanding of the practical strategies employed in dynamic cybersecurity environments. Tingare et al. (2024) reported that pragmatic inquiry allowed flexible methods and supported the integration of diverse data sources to produce actionable results. Such characteristics positioned pragmatic inquiry as the most appropriate approach for examining how data managers in Virginia, Maryland, and DC applied breach-management strategies.

Pragmatic inquiry offered more substantial alignment with the study's goals than other qualitative designs. Phenomenology focused on lived experience, which did not support an action-oriented approach. Grounded theory aimed to generate a new theory, which did not match the goal of examining existing practices supported by CRMT and SCCT. Ethnography required long-term cultural immersion, which did not fit the

business-centered context of the study. A case study required extensive organizational documentation, which did not align with the need for cross-organizational comparison. Houghton (2023) emphasized that pragmatic inquiry supported flexible logic, mixed methods, and practical outcomes grounded in participant insight. Such strengths established pragmatic inquiry as the most fitting design for the research.

Data saturation occurred once no new insights emerged from the last participant responses. Hennink et al. (2022) stated that saturation occurred when additional data failed to generate new ideas. Participants repeated strategies involving training, proactive controls, communication, and structured responses, which confirmed saturation. Weyant (2022) noted that saturation occurred more consistently when participants held strong knowledge of the topic. Such conditions aligned with the purposeful sampling strategy used in the study.

Semistructured interviews and document analysis strengthened methodological rigor and supported the pragmatic inquiry design. Braun and Clarke (2021) reported that using multiple data sources increased the trustworthiness of findings by validating them across different evidence types. Triangulation enhanced the reliability of the themes and ensured an accurate reflection of real breach-management practices. The use of a pragmatic inquiry design yielded findings that were practical, relevant, and grounded in the participants' experiences.

## **Population and Sampling**

### **Population**

Eligible participants held roles as data managers, cybersecurity leaders, or professionals directly responsible for overseeing data breach response and management. All participants had a minimum of 2 years of experience in cybersecurity incident handling and worked within one of the designated geographic regions: Washington, D.C., Maryland, or Virginia. These criteria ensured that participants possessed firsthand knowledge relevant to the study's objectives. I selected these sectors because they frequently experience data breaches and operate under regulatory mandates that require stringent data protection. Spanca et al. (2024) explained that organizations in these industries faced unique challenges in both security and consumer trust restoration, making their perspectives indispensable for this study. To recruit participants, I drew from my professional networks, cybersecurity associations, and LinkedIn. I distributed formal email invitations that outlined the study's purpose, eligibility requirements, and the expected time commitment. I also networked through cybersecurity forums and regional conferences across Washington, DC; Maryland; and Virginia to broaden outreach.

### **Sampling**

I employed purposeful sampling to select participants who possessed the expertise and relevance necessary to address the research question. Purposeful sampling allowed me to identify individuals whose professional experiences directly aligned with the topic (Weyant, 2022). This method ensured that each participant contributed valuable, context-

rich insights into data breach management and the recovery of consumer trust. Weyant (2022) supported this approach for qualitative studies seeking to capture expert perspectives rather than statistical generalizations.

The final sample consisted of 10 data managers, an optimal size for qualitative inquiry that aims to achieve data saturation. Hennink et al. (2022) explained that smaller samples often achieve saturation when researchers select participants for their expertise and relevance. Weyant (2022) also noted that studies with 10–12 participants typically yielded comprehensive data while maintaining manageability. I chose this sampling method to ensure participants possessed substantive experience in managing data breaches. Abdullah et al. (2025) emphasized that financial, health care, retail, and government sectors were particularly vulnerable due to the sensitivity of their operations, making expert insight critical. Purposeful sampling guaranteed that the data reflected real-world challenges and strategies within high-risk industries.

### **Ethical Research**

I followed ethical research standards to protect all participants in this study. I used an informed consent process that allowed each participant to review the study's purpose, the voluntary nature of participation, and the procedures involved. Participants received the informed consent form prior to the interviews and had the opportunity to ask questions. I allowed participants to withdraw from the study at any time and for any reason. Participants could withdraw by email, by phone, or verbally during the interview. I informed each participant that withdrawal would result in the destruction of all collected data related to that individual. I did not offer incentives for participation. Weyant (2022)

stated that voluntary participation without incentives supported trust and reduced concerns about undue influence. This approach aligned with the ethical guidelines used in qualitative studies.

I applied several measures to ensure adequate protection of participants. I used secure digital storage, encrypted files, and password-protected devices. Braun and Clarke (2021) explained that secure handling of qualitative data strengthened confidentiality and improved ethical integrity. I removed all identifying information from transcripts to protect anonymity. I used pseudonyms for each participant and assigned general labels for organizations. These steps prevented the disclosure of personal identities and organizational names. All 10 participants signed the informed consent form before participating in the interview. I stored all research data in secure digital folders. I will keep all data for 5 years, as required, to protect participant confidentiality. After 5 years, I will permanently delete all files.

I maintained confidentiality throughout the study. I protected the names of individuals and organizations by removing identifying details and using neutral descriptors in all written materials. This process aligned with ethical standards for minimizing risk and safeguarding participants. Driggers and Boyles (2024) stated that ethical protection improved trust and supported high-quality data collection in qualitative studies. These practices ensured that participants contributed their insights safely and without risk of exposure. The Walden University Institutional Review Board approval number for this study is 05-30-25-1166266.

### **Data Collection Instruments**

I served as the primary data collection instrument for this qualitative study. I collected data through semistructured interviews and document analysis. Weyant (2022) explained that semistructured interviews encouraged open discussion while maintaining the conversation's alignment with the research question. Braun and Clarke (2021) stated that document analysis added context and strengthened the quality of qualitative data. I used an interview protocol to guide each of the interviews (see Appendix). I opened each interview with an introduction, explained the confidentiality policy, and asked the predetermined open-ended questions. I followed the same protocol for every participant to maintain consistency. I used probing questions when I needed clarification or a deeper explanation.

I strengthened the reliability and validity of the data collection process by incorporating member checking. I conducted member checking by scheduling an interview with participants to ask them to verify the accuracy of their statements, clarify ambiguous points, and confirm that I reflected their intended meaning. Driggers and Boyles (2024) emphasized that this type of participant confirmation increased trust and reinforced the strength of qualitative results. During my interview with participants, I engaged in real-time member checking by summarizing key points and asking participants to confirm or correct my interpretations. Braun and Clarke (2021) noted that systematic verification during data collection increased the credibility of qualitative findings.

I protected all data through secure procedures. I recorded interviews with the participants' consent and stored the audio files and transcripts in encrypted, password-protected folders. These actions aligned with recommendations from recent qualitative scholars and ensured that the instruments and procedures produced accurate and trustworthy data.

After completing the project, I applied several methods to enhance the reliability and credibility of the findings. I employed member checking, bracketing, immersion, and audit trailing to mitigate researcher bias and validate interpretations. Amin et al. (2020) asserted that these techniques strengthened trustworthiness by ensuring that researchers accurately and transparently represented the views of participants. These techniques also enhanced dependability by establishing a systematic process for reflection and validation.

I conducted semistructured interviews as the primary data collection method, which allowed participants to share their experiences freely while ensuring alignment with the study's objectives. I supplemented these interviews with secondary data from reputable sources, including cybersecurity reports, government publications, and industry case studies. This triangulation approach provided context, validated findings, and broadened the study's scope. Using authoritative sources—such as federal agencies, cybersecurity firms, and professional associations—ensured credibility and alignment with the best practices of qualitative research. I contacted participants to review my interpretations of their statements and confirm the accuracy of the captured meaning. I corrected any identified discrepancies, ensuring that the final results reflected participants' intended perspectives.

Yin (2018) stated that semistructured interviews strike a balance between flexibility and structure, making them ideal for qualitative inquiry. I anonymized all interview data to protect participants' identities and maintained strict confidentiality throughout the research process. I adhered to all ethical guidelines and methodological rigor to mitigate bias, ensuring that the study contributed valuable insights into managing data breaches and restoring consumer trust.

### **Data Collection Technique**

I collected data through semistructured interviews and followed a structured, step-by-step process. I began each interview by greeting the participant, reviewing the study's purpose, and explaining the principles of confidentiality, voluntary participation, and the option to stop the interview at any time. I asked open-ended questions from the interview protocol and used probing questions when clarification was necessary. I recorded each interview with participant consent and took brief supporting notes. Semistructured interviews allowed focused yet flexible discussions. Weyant (2022) explained that this approach enabled participants to describe their experiences in depth while still aligning with the research question. Braun and Clarke (2021) emphasized that semistructured interviews supported meaningful insights because participants could elaborate on their perspectives. These advantages made interviews an appropriate method for collecting data in this study.

Semistructured interviews also required careful attention to time and focus. Participants occasionally offered lengthy or divergent responses, which required refocusing the discussion. Weyant (2022) noted that semistructured interviews demanded

strong researcher attention to keep conversations aligned with the research purpose. I also maintained scheduling flexibility because participants lived across Washington, D.C., Maryland, and Virginia. I did not conduct a pilot study because the interview questions aligned well with the research purpose and reflected established standards in qualitative interviewing. To meet Walden's requirements for validating qualitative data, I used member checking. I contacted the participants to verify the accuracy of their statements, clarify unclear sections, and confirm that I captured their intended meaning. Driggers and Boyles (2024) noted that reviewing responses with participants strengthened accuracy and increased participant trust. I performed member checking by contacting the participant by telephone to review the accuracy of each response.

I also double-checked my data interpretation during the interviews. As participants shared key points, I summarized their statements in real time and asked them to confirm, expand, or correct my interpretation. Braun and Clarke (2021) explained that this type of systematic verification improved the credibility of qualitative findings. These two strategies, real-time clarification and member checking, after I completed organizing responses, ensured that my interpretations accurately reflected the participants' perspectives.

I relied solely on semistructured interviews for primary data collection and did not use any documents, archival records, or public websites as supplemental data sources. I secured all audio recordings, transcripts, and notes in encrypted, password-protected folders to protect confidentiality. This data collection technique produced rich

descriptions that supported the identification of strategies data managers used to manage data breaches and restore consumer trust.

### **Data Organization Techniques**

Effective data organization was crucial for collecting, managing, and securing data while upholding ethical standards. In this research, I employed thematic analysis to uncover key themes that addressed the central research question. Braun and Clarke (2021) described thematic analysis as a structured process of identifying, analyzing, and reporting patterns within qualitative data. This approach provided a rich and nuanced understanding of participants' experiences. Pearson et al. (2025) explained that thematic analysis required researchers to familiarize themselves with the data, generate initial codes, organize these codes into themes, and refine them to ensure accuracy and representativeness.

To streamline data management, I leveraged modern tools and technologies. I collected all interview transcripts, audio recordings, and relevant supporting documents, assigning pseudonyms such as "Participant 1" and "Participant 2" to protect participant anonymity. I stored these materials securely in cloud-based platforms, including iCloud and Google Drive, ensuring confidentiality and accessibility. I also maintained an encrypted backup on a password-protected external hard drive stored in a locked, secure location, consistent with best practices in data protection.

To enhance organization, I developed a comprehensive data catalog that recorded each data source, its collection date, and storage location. This catalog facilitated the efficient import of materials into NVivo software for coding and analysis. NVivo's AI-

assisted tools, including automated transcription and pattern recognition, supported efficient categorization and visualization of themes (Allsop et al., 2022). These features enhanced the analytical process by improving consistency and accuracy when identifying recurring patterns and relationships within the data set. After transcribing and coding the data, I conducted member checking to validate the credibility of my findings. I contacted each participant to review his or her response to each question. This verification process strengthened the credibility and trustworthiness of the study (Hayden et al., 2023).

As the researcher, I personally conducted the thematic analysis to ensure that all emerging themes originated directly from the data. NVivo assisted in organizing, verifying, and visualizing the coded material, but did not perform the analysis. I used NVivo's visualization tools—such as heatmaps and network diagrams—to display relationships among codes and themes, which clarified and enhanced the interpretation of findings.

Data security remained a top priority throughout the research process and continued to be a priority after its completion. Upon completing the study, I shredded all hard-copy documents and permanently deleted electronic records from both cloud and local storage following a 5-year retention period, in accordance with ethical research standards (Toombs et al., 2025). By employing these systematic data organization and analysis methods, I ensured that the study was conducted with rigor, transparency, and integrity while utilizing technology to improve the accuracy and efficiency of qualitative analysis.

## **Data Analysis**

I began the data analysis process immediately after conducting the first interview, as recommended by Berret and Munzner (2025), which allowed for real-time adjustments to the sampling and methodology. I applied Braun and Clarke's (2021) six-phase framework for thematic analysis. I first familiarized myself with the data by reading and rereading transcripts to gain a deep understanding of the content, noting initial impressions and observations. Next, I generated initial codes by systematically examining the data and identifying significant statements and patterns related to the research questions (Braun & Clarke, 2021). I labeled these segments concisely to capture the meaning of participants' responses. I then grouped the codes into potential themes, identifying relationships among them, and organizing them into meaningful categories. After developing preliminary themes, I reviewed and refined them to ensure they accurately represented the coded data and reflected the overall data set.

Once I finalized the themes, I defined and named each one to reflect its scope and significance (Braun & Clarke, 2021). I then produced a comprehensive report that detailed each theme, incorporating direct quotations from participants to illustrate their perspectives. This narrative effectively conveys how the findings address the research question and connect to the study's conceptual frameworks. To ensure credibility, I used member checking as a key verification strategy. After completing transcription and coding, I contacted the participants to review my interpretations of their responses to confirm that the analysis accurately reflected their experiences. Their feedback validated the accuracy and authenticity of my findings, reinforcing the study's trustworthiness.

I maintained data integrity by transcribing the audio recordings verbatim, capturing pauses, hesitations, and relevant nonverbal expressions. I reviewed each transcript against the original recording to verify accuracy and correct any inconsistencies. Once finalized, I formatted the transcripts for analysis by organizing responses according to interview questions, numbering lines for easy reference, and anonymizing participant information to preserve confidentiality. As the primary researcher, I performed the thematic analysis manually, ensuring that all interpretations remained grounded in the data. NVivo served as an analytical support tool that helped me organize, verify, and visualize data. I utilized NVivo's heatmaps and network diagrams to identify interrelationships and trends within the coded material, while I made all analytical and interpretive decisions independently to ensure methodological rigor. To uphold transparency and reliability, I maintained a detailed audit trail documenting analytical decisions, coding justifications, and member-checking feedback. Before finalizing the findings, I conducted a quality assurance review to ensure that all identified themes consistently aligned with the data set. This structured and transparent process reinforced the study's dependability and validity.

I also applied methodological triangulation by integrating data from semistructured interviews with verifiable public documents and professional reports, as advocated by Vivek et al. (2023). I utilized publicly available resources, including organizational cybersecurity policies, federal regulatory guidance, industry breach reports, and reputable cybersecurity frameworks, to support and contextualize the interview findings. I reviewed documents that included agency cybersecurity guidelines,

publicly posted data breach notifications, annual cybersecurity reports from recognized professional associations, and federal cybersecurity compliance publications. These materials helped me confirm patterns, compare reported practices with established standards, and strengthen the credibility of the study through multiple sources of evidence. This approach enriched the findings by allowing cross-validation across multiple sources. I compared organizational records, public statements, and interview data to strengthen reliability and provide a holistic understanding of how data managers addressed cybersecurity threats. Ohneberg et al. (2022) emphasized that triangulation enhances credibility and reduces the likelihood of interpretive bias.

NVivo software supported the management and organization of large volumes of qualitative data during thematic analysis. Peel (2020) noted that using NVivo allowed researchers to categorize and structure qualitative data systematically. I followed Linneberg and Korsgaard's (2019) guidance in developing codes that maintained alignment with the research question and accurately captured participants' nuanced responses. Additionally, I used color coding to distinguish themes and patterns, as suggested by Rahman et al. (2024), which helped maintain close engagement with participants' words and enhanced interpretive clarity. By integrating rigorous thematic analysis, triangulation, and technological support, I ensured that the data analysis process was transparent, systematic, and methodologically sound. This approach produced credible insights into how data managers in Virginia, Maryland, and DC managed data breaches and restored consumer trust in digital platforms.

## **Reliability and Validity**

I took different actions to establish reliability and validity in this qualitative study. Unlike quantitative studies, qualitative research relies on credibility, transferability, dependability, and confirmability to ensure trustworthiness. I enhanced reliability and credibility through member checking and methodological triangulation. During member checking, I invited participants to review my interpretations of their responses and confirm that my analysis accurately reflected their intended meanings. I strengthened transferability by providing rich, detailed descriptions that enable future researchers to determine whether the findings can apply to different contexts. I achieved data saturation by collecting and analyzing data until no new themes or insights emerged. These approaches aligned with the best practices of qualitative research, reinforcing the integrity and trustworthiness of the findings.

### **Reliability**

*Reliability* in qualitative research refers to the consistency and dependability of the findings (Spiers et al., 2021). Reliable research demonstrated that data collection and analysis procedures consistently aligned with the evidence gathered from participants. I ensured reliability by systematically monitoring and refining the research process throughout the project. Yin (2018) emphasized that maintaining reliability required researchers to critically evaluate their methodological decisions, while Egan et al. (2023) underscored the importance of using dependable data collection instruments that influenced both reliability and validity.

In this project, I ensured reliability by employing semistructured interviews and document analysis. This combination enabled me to thoroughly explore data breach management while minimizing research bias. I applied a structured interview protocol (see Appendix) and asked each participant the same set of questions to maintain consistency (Yin, 2018). Motulsky (2021) recommended using mechanical recording, member checking, and collecting rich data to enhance reliability; I integrated each of these techniques to ensure accuracy and transparency during data collection.

*Dependability* refers to the stability, consistency, and repeatability of the research process, ensuring that another researcher could follow the same procedures and arrive at comparable findings. To reinforce dependability, I used member checking as a key validation technique. I contacted participants to review my interpretations of their responses and confirm that my analysis accurately captured their perspectives (Alifia et al., 2025). This process allowed participants to clarify or elaborate on their intended meanings, ensuring alignment between their experiences and my interpretations. Incorporating member checking enhanced both credibility and reliability, confirming that the findings reflected participants' authentic viewpoints.

I conducted interviews until I reached data saturation, which occurred when no new information or themes emerged. Naeem et al. (2024) emphasized that achieving saturation demonstrated that the data provided adequate support for the conclusions. I continued collecting and reviewing data until saturation occurred, ensuring that the findings were comprehensive and well-substantiated. I also strengthened reliability through triangulation by gathering information from multiple sources, including

semistructured interviews, public documents, and organizational reports. Methodological triangulation enabled me to corroborate findings, mitigate potential bias, and develop a comprehensive understanding of data breach management and consumer trust (Pearson et al., 2025). By using structured interview protocols, incorporating member checking, seeking expert validation, ensuring data saturation, and applying triangulation, I established a dependable and credible foundation for the study. These strategies provided a rigorous framework for examining how data managers addressed data breaches and preserved consumer trust in digital environments.

### **Validity**

In the context of data breach management, validity requires that the findings accurately represent participants' experiences and the strategies they used to restore consumer trust. I established validity in this study by ensuring credibility, transferability, and confirmability, three essential components of trustworthiness in qualitative research (Abu et al., 2023). Credibility ensured that the data authentically reflected participants' lived experiences (Rose & Johnson, 2020). I enhanced credibility by conducting member checking, during which I shared my preliminary interpretations with participants to verify their accuracy. This process confirmed that my findings captured participants' perspectives and provided an accurate portrayal of their approaches to managing data breaches.

Transferability referred to the extent to which the findings could apply to other contexts or organizations, a key dimension of qualitative trustworthiness described by Braun and Clarke (2021). I achieved transferability by providing detailed descriptions of

the research setting, participants, and conditions. I also included accounts of data breach management practices among business leaders in Virginia, Maryland, and DC. These descriptions covered several industries, including financial services, government, and e-commerce. These detailed contextual descriptions enabled other researchers and practitioners to assess the applicability of the findings to their own settings, thereby enhancing the broader relevance and utility of the research (Rouse et al., 2025).

Confirmability ensured that the findings were grounded in participants' input rather than influenced by researcher bias (Berret & Munzner, 2025). I maintained confirmability by keeping a detailed audit trail documenting every stage of the research process, including methodological decisions, coding rationales, and member-checking results. I used NVivo software to assist with organizing and verifying data, ensuring that the themes emerged directly from participant evidence rather than being subject to subjective interpretation (Allsop et al., 2022).

Finally, I validated the study's findings through data saturation, which occurred once no new insights emerged from the interviews or document analysis (Weyant, 2022). I continued data collection until I achieved saturation. This approach ensured completeness, reliability, and alignment with the study's purpose. I also used member checking, triangulation, and an audit trail. These strategies helped the study achieve high credibility, transferability, dependability, and confirmability. These measures strengthened the overall trustworthiness of the research and reinforced its contribution to understanding data breach management and the restoration of consumer trust.

## **Transition and Summary**

In this qualitative, pragmatic inquiry, I explored the strategies employed by data managers in Virginia, Maryland, and DC to manage data breaches and restore consumer trust in digital platforms. In Section 1, I reviewed professional and academic literature emphasizing the relevance of CMT and the RMF. These frameworks can guide organizational leaders in developing preventive measures and post-breach recovery strategies to minimize the long-term effects of data breaches on consumer trust and business continuity.

In Section 2, I described the essential components of the research methodology, including the rationale for choosing a qualitative design, the criteria for participant selection, and the ethical standards that governed the study. I explained the data collection process, which incorporated semistructured interviews and document analysis, and detailed the organizational and analytical techniques applied. To enhance trustworthiness, I incorporated member checking and triangulation, ensuring that the findings accurately reflected participants' perspectives and experiences.

In Section 3, I present the research findings organized around the central themes identified during the analysis. I discuss how these findings contributed to professional practice by offering practical recommendations for improving data breach management and rebuilding consumer confidence. I also explore the implications for social change, highlighting how effective data breach management promotes organizational transparency and strengthens public trust. Finally, I provide recommendations for future

research, reflected on my experiences as a researcher, and concluded the study with a summary of key insights and contributions.

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

The purpose of this qualitative, pragmatic inquiry was to explore the practical strategies that data managers employed to manage data breaches and restore consumer trust in digital platforms. In this section, I apply the study's findings to professional practice and explored their broader implications for social change. The intent is to connect the study's results to actionable strategies that business leaders could implement to strengthen cybersecurity practices, enhance consumer confidence, and promote the operational resilience of digital organizations.

The findings revealed that effective data breach management required preparation, coordinated response, and sustained resilience. Participants emphasized that education and continuous training reduced vulnerabilities by equipping personnel to recognize phishing attempts, detect insider threats, and protect sensitive information. By empowering employees to assume ownership of data security responsibilities, organizations strengthened both accountability and preparedness across all operational levels. Participants also underscored the critical role of communication and collaboration. They explained that involving data owners, cybersecurity teams, executive leadership, and system managers in coordinated response activities ensured consistency, transparency, and efficiency. Maintaining open and transparent communication within the organization, as well as with external stakeholders, helped preserve confidence during and after breach incidents. Incident response protocols served as the foundation for timely recovery. Participants implemented structured frameworks supported by proactive measures, including tabletop exercises, failover testing, and backup validation. Rapid

forensic analysis and swift containment minimized potential damage while guiding the implementation of corrective actions.

Participants also emphasized the importance of incorporating internal controls and cybersecurity requirements into the early stages of acquisition and system design processes. They asserted that integrating controls into the procurement and development stages proved far more effective than implementing safeguards retroactively after a breach occurred. Leadership adaptation emerged as another critical factor in crisis management. While transformational leadership fostered long-term cultural change and resilience, participants adopted transactional methods during crises—such as defining clear roles, delegating specific tasks, and providing targeted incentives—to ensure disciplined execution under pressure. Maintaining communication channels and enforcing established protocols remained central to leadership accountability during breach response.

Finally, participants identified trust and reputation management as persistent organizational challenges. Government agencies often addressed public trust less directly than private entities; however, all participants agreed that restoring confidence in institutional practices was essential to sustaining credibility and ensuring mission success. Overall, the findings demonstrated that preparedness, collaboration, structured protocols, integrated controls, adaptive leadership, and deliberate trust restoration constituted the essential elements of effective data breach management. These practices not only supported immediate recovery but also contributed to long-term organizational resilience and public confidence in digital ecosystems.

## **Presentation of the Findings**

The overarching research question for this study asked, What strategies did data managers employ to manage data breaches and improve consumer trust in digital platforms? The analysis of 10 participant interviews revealed five major themes: (a) education and training, (b) communication and collaboration, (c) structured incident response, (d) proactive integration of controls, and (e) leadership and trust management. The findings collectively demonstrated that participants implemented proactive education programs, emphasized cross-functional collaboration, adopted standardized incident response frameworks, integrated cybersecurity controls early in system development, and prioritized trust restoration as part of their organizational recovery process. Each participant contributed perspectives that aligned with the conceptual frameworks—CRMT and SCCT—which reinforced the study’s theoretical foundation and practical relevance. Table 1 shows the words and phrases used by the 10 participants that relate to each identified theme.

### **Theme 1: Education and Training**

All 10 participants emphasized that continuous education and training were central to preventing data breaches and strengthening organizational resilience:

- Participant 1 emphasized cybersecurity awareness programs tailored to identify phishing attempts and mitigate insider threats.
- Participant 2 highlighted the use of continuous skill development programs to enhance technical readiness and response capability.

- Participant 3 described mandatory cybersecurity certifications and refresher courses to promote compliance and accountability.
- Participant 4 stated that integrating cybersecurity modules into employee onboarding established a foundation for security culture early in employment.
- Participants 5–9 echoed similar perspectives, noting that regular training and simulated breach exercises enhanced awareness across departments and reduced the likelihood of human error.

The participants described these initiatives as both preventive and developmental. They agreed that workforce education empowered employees to act as the first line of defense against cyber threats and ensured compliance with regulatory requirements. These findings aligned with Zhu and Wang (2025), who concluded that continuous workforce training remained one of the most effective safeguards against breaches. Participants confirmed that organizations that invested in training not only reduced vulnerabilities but also cultivated accountability, vigilance, and a culture of security ownership.

## **Theme 2: Communication and Collaboration**

All participants consistently emphasized the importance of communication and collaboration as critical components of successful breach management:

- Participant 1 emphasized rapid escalation and coordination with internal teams and oversight entities.

- Participant 2 detailed the importance of maintaining direct communication with incident response and compliance officers to ensure real-time updates.
- Participant 3 explained that aligning data owners, legal staff, and system administrators fostered transparent reporting and accountability.
- Participant 4 highlighted the value of structured communication channels that minimized confusion during critical response windows.
- Participants 5–9 added that collaboration between cybersecurity professionals, leadership, and external partners enabled timely containment and recovery.

Several participants shared that unclear communication led to delays and inconsistencies, reinforcing the need for structured collaboration frameworks. They collectively agreed that proactive communication not only mitigated reputational damage but also preserved organizational credibility. These findings align with those of L. Kim (2021) and Q. Zhu et al. (2024), who emphasized that transparent communication and cross-functional teamwork accelerate trust recovery and minimize operational disruptions.

### **Theme 3: Structured Incident Response**

Participants 1 through 9 emphasized the importance of establishing and applying structured incident response frameworks as essential to effective breach management:

- Participant 1 referred to adherence to the National Institute of Standards and Technology (NIST) and SANS Institute (SANS) incident response models,

emphasizing the importance of swift detection, classification, and escalation protocols.

- Participants 2 and 3 described implementing backup validation, tabletop exercises, and after-action reviews to test preparedness and evaluate procedural efficiency.
- Participant 4 underscored the use of containment checklists and incident logs to maintain audit readiness.
- Participants 5–9 reiterated that response discipline and predefined escalation paths limited both operational and reputational losses.

Participants collectively described structured response frameworks as a means to institutionalize resilience. Continuous simulations and readiness assessments enabled the refinement of procedures and the early identification of weaknesses before actual incidents occurred. These findings confirm those of Hoehle et al. (2022), who asserted that formalized response structures reduce response time and minimize systemic impact. The participants demonstrated that integrating incident response testing and validation served as both a preventive and corrective strategy in safeguarding organizational stability.

#### **Theme 4: Proactive Integration of Controls**

Participants consistently emphasized the importance of integrating cybersecurity controls into the system acquisition and design phases, rather than relying on reactive measures:

- Participants 1–4 emphasized that embedding security requirements early in procurement processes prevented vulnerabilities and reduced future compliance costs.
- Participants 5 and 6 noted that control integration during the acquisition phase ensured adherence to frameworks such as Department of Defense Manual 5400.11 and Office of Management and Budget M-17-12.
- Participants 7–9 reinforced that proactive control implementation reduced vendor-related risks and eliminated the need for post-incident retrofits.

This approach aligns with Tingare et al. (2024), who advocated for a preventive shift in cybersecurity management practices. Participants explained that integrating controls at the design level enhanced accountability and compliance while reducing the likelihood of long-term systemic failures. The evidence supported the argument that preventive integration offered a cost-effective and sustainable solution to organizational security management.

### **Theme 5: Leadership and Trust Management**

All 10 participants identified leadership and trust management as pivotal to effective data breach response:

- Participant 1 discussed employing transformational leadership to foster accountability and ethical behavior during crisis events.
- Participant 2 emphasized the importance of transparent leadership communication in reinforcing organizational credibility.

- Participant 3 described leadership’s responsibility to model cyber-safe behavior and ensure psychological safety for employees following a breach.
- Participant 4 combined transactional leadership—assigning roles and defining expectations—with transformational culture-building to motivate performance.
- Participants 5–9 collectively agreed that restoring consumer and stakeholder trust required sustained engagement, empathy, and demonstrated competence over time.

Participants noted that while private sector organizations measured trust through customer metrics, government agencies emphasized mission performance and public transparency. These perspectives were also extended to Nikkhah and Grover (2024), who highlighted that reputational recovery often outlasts technical remediation. The participants confirmed that leadership effectiveness, visibility, and authenticity directly influenced trust restoration and institutional resilience. Table 2 shows commonly recurring words and phrases in participant interviews. The words and phrases are organized by theme.

**Table 2**

*Recurring Words and Phrases Identified Across Participant Interviews*

Theme	Commonly recurring words/phrases	<i>f</i> across the 10 participants
Education and training	“Phishing,” “awareness,” “continuous learning,” “human error,” “accountability,” “training programs”	9
Communication and collaboration	“Coordination,” “reporting,” “transparency,” “battle rhythm,” “teamwork,” “real-time updates	9

Structured incident response	“NIST,” “SANS,” “containment,” “forensics,” “response framework,” “simulation”	8
Proactive integration of controls	“Early controls,” “procurement,” “preventive measures,” “built-in security,” “compliance frameworks”	7
Leadership and trust management	“Leadership,” “accountability,” “reputation,” “trust,” “culture,” “restoration”	9

*Note.* Frequency represents the number of participants referencing each term or a conceptually equivalent phrase during the interviews. NIST = National Institute of Standards and Technology.

### **Synthesis of the Findings**

The findings confirm that effective data breach management required a comprehensive approach encompassing technical, procedural, and leadership dimensions. Participants demonstrated that organizations that invested in education, standardized communication, structured response systems, and proactive control integration developed stronger resilience and faster recovery trajectories. These findings align with CRMT, which emphasizes risk identification, mitigation, and the adoption of proactive controls (Mann, 2024). They also supported the SCCT, which emphasizes that transparent communication and stakeholder engagement are essential to restoring public confidence (Coombs, 2007).

The study extends the prior literature (Aslam et al., 2022; X. Chen et al., 2022; Kochetkov, 2024) by revealing that the early integration of controls within acquisition cycles and adaptive leadership practices represents emerging best practices in digital trust

recovery. No findings contradicted existing research; however, differences between public- and private-sector trust restoration approaches highlighted an underexplored area of study. Overall, the 10 participants collectively demonstrated that integrating cybersecurity strategies with ethical leadership and transparent crisis communication transformed breach management from a reactive process into a proactive, trust-centered discipline. These results provide actionable insights for data managers and policymakers seeking to strengthen resilience and sustain public confidence in the digital era.

The documents and supporting materials revealed several patterns that reinforced and extended the findings from the interview. The National Institute of Standards and Technology (NIST, 2018) cybersecurity framework and related federal directives emphasize the importance of early control integration, continuous monitoring, and structured incident response, which align closely with participants' descriptions of effective breach management. Federal Trade Commission breach notification records illustrated real-world consequences of delayed reporting and insufficient crisis communication, highlighting the practical value of the rapid disclosure practices described by participants. Industry analyses, including the IBM Cost of a Data Breach Report and cybersecurity assessments from professional associations, consistently demonstrate that organizations with proactive governance practices, trained personnel, and transparent communication strategies recover trust more quickly and reduce long-term financial impact. These materials validated the strategies identified in the interviews, confirmed alignment with recognized best practices, and revealed a broader

trend toward embedding cybersecurity governance, ethical leadership, and trust-centered communication within organizational culture.

### **Applications to Professional Practice**

The findings of this study have significant implications for professional business practice, particularly for organizations seeking to strengthen digital resilience, preserve consumer trust, and mitigate the financial consequences of data breaches. The 10 participants emphasized that proactive cybersecurity strategies, transparent communication, and post-breach remediation practices were essential components of organizational resilience. Their collective insights demonstrated that effective breach management required not only technical solutions but also strong leadership, structured protocols, and a culture of accountability and trust. These findings aligned with and extended the literature on CRMT and SCCT by illustrating how both frameworks integrated seamlessly into modern cybersecurity management practices.

### **Education and Training as a Preventive Strategy**

Participants emphasized that ongoing education and training programs formed the foundation of cybersecurity resilience. Ten participants with experience managing data breaches in complex digital environments agreed that employees served as the first line of defense against cyber threats. Participants explained that workforce education reduced human error and enhanced situational awareness. They described how continuous training in phishing identification, insider threat detection, and data handling practices reinforced compliance and accountability across departments. Participant 1 stressed that “education reduced fear and confusion during incidents,” while Participant 3 emphasized

that “training transformed cybersecurity from a technical issue to an organizational value.” These findings confirmed that embedding cybersecurity education into corporate culture improved both readiness and response effectiveness.

### **Communication and Collaboration as Operational Cornerstones**

Participants identified communication and collaboration as operational imperatives that enhanced trust and accelerated recovery. They described how coordinated communication among cybersecurity teams, leadership, and external stakeholders allowed organizations to respond quickly and transparently. Participant 2 explained that “consistent updates prevented misinformation,” while Participant 5 observed that “communication alignment among departments minimized confusion and improved decision-making.” The participants agreed that communication breakdowns delayed containment and prolonged reputational harm. Participant 8 noted that transparent communication with vendors and consumers demonstrated ethical responsibility, which restored trust. These insights illustrated how SCCT principles—emphasizing clear, timely, and honest communication—remained critical for managing public perception and protecting institutional credibility after a breach.

### **Structured Incident Response as a Core Capability**

All 10 participants emphasized that structured incident response frameworks served as the backbone of effective cybersecurity management. They described adopting established models such as the NIST Cybersecurity Framework and the SANS Incident Response Model to ensure consistency, traceability, and accountability. Participant 4 emphasized that “using a tested framework eliminated guesswork during crisis response,”

while Participant 6 added that “standard operating procedures kept everyone aligned under pressure.” Participants 7 and 9 emphasized that regular tabletop exercises and backup validation reinforced readiness and prevented escalation. The findings confirmed those of Hoehle et al. (2022), who noted that formalized response mechanisms minimize operational downtime and financial loss. By integrating structured frameworks into organizational operations, participants demonstrated how preparation directly improved recovery efficiency and post-incident learning.

### **Proactive Integration of Controls for Sustainable Defense**

Participants highlighted that embedding cybersecurity control early in system development and acquisition processes provided long-term protection. Participants 1 through 10 consistently agreed that early integration of controls during procurement, rather than retroactive correction, reduced exposure to vulnerabilities and compliance risks. Participant 6 emphasized that “controls built into the design phase prevented costly remediation later,” and Participant 9 confirmed that “security baked in early saved both time and reputation.” These proactive measures aligned with Garba et al. (2023), who advocated for a shift from reactive to preventive cybersecurity management. The findings also extended CRMT, which emphasized risk anticipation, mitigation, and integration into governance processes. By embedding security into acquisition lifecycles, participants reinforced that cybersecurity effectiveness depended on foresight rather than reaction.

### **Leadership and Trust Management as Strategic Imperatives**

All participants identified leadership as the most influential factor in managing data breaches and restoring stakeholder trust. They described leadership as both

situational and transformational, depending on the stage of the crisis. Participant 3 emphasized that “leaders who demonstrated transparency earned credibility,” while Participant 4 stated that “consistent leadership communication maintained calm and cohesion.” Participants 5 and 7 noted that leadership accountability has a direct influence on employee morale and public confidence. Participants 8 and 9 explained that private sector organizations often used customer feedback and sentiment analysis to measure trust, while government leaders focused on maintaining public transparency and mission reliability. These findings support Mishra et al. (2022), who observed that reputational recovery requires a long-term commitment beyond technical remediation. The leader’s ability to balance technical action with human connection emerged as the defining factor in rebuilding organizational reputation and trust.

### **Key Insights From the Findings**

The findings demonstrate that data breach management was not confined to technical cybersecurity but constituted a strategic organizational function that merged human behavior, leadership, and governance. Organizations that implemented comprehensive cybersecurity programs, integrated early control measures, and sustained open communication experienced stronger operational continuity and public trust. The participants’ real-world experiences validated that CRMT and SCCT, when applied jointly, enhanced risk preparedness and ethical response management.

CRMT guided organizational leaders to identify vulnerabilities early, embed controls at every stage, and manage risks systematically. SCCT complemented this approach by ensuring that leaders communicated with empathy, transparency, and

accountability, thereby protecting organizational reputation. Together, these frameworks formed a robust model for addressing both the technical and relational aspects of data breach recovery.

Participant insights also demonstrated that cybersecurity investments generated returns beyond compliance—they preserved brand integrity, improved stakeholder engagement, and reduced the overall cost of crisis response. Organizations that adopted these practices established themselves as trustworthy custodians of data and ethical stewards of technology.

The application of these findings to professional practice underscore five enduring principles:

- Investing in cybersecurity education cultivates awareness, competence, and accountability.
- Establishing communication protocols ensures transparency, minimized confusion, and fostered confidence among stakeholders.
- Maintaining structured incident response systems accelerates containment and recovery.
- Integrating preventive controls into procurement and design processes reduce long-term risk exposure.
- Exercising adaptive leadership sustains trust, credibility, and organizational resilience.

By adopting these strategies, business leaders could strengthen their organization's digital trust framework, comply with regulatory standards, and transform data breach management into a proactive driver of long-term competitiveness and ethical excellence.

### **Implications for Social Change**

The findings of this study have important implications for social change by demonstrating how effective data breach management strategies protected individuals, communities, organizations, and societies from the adverse consequences of cyber incidents. The 10 participants with significant leadership and data management experience shared strategies that extended beyond technical response to ethical responsibility, transparency, and restoration of public trust. Their collective insights revealed that organizations that managed breaches responsibly not only strengthened operational resilience but also advanced digital equity, consumer confidence, and societal well-being.

#### **Individual Level: Protecting Privacy and Restoring Trust**

At the individual level, participants confirmed that improved breach management practices enhanced the protection of personal and financial information. Participant 1 emphasized that rapid response procedures “helped individuals recover their sense of safety after exposure,” while Participant 6 noted that “transparent communication reduced fear and confusion for affected users.” These findings illustrated that effective data breach responses preserved personal privacy and human dignity in digital spaces.

By implementing proactive safeguards and clearly communicating post-breach actions, organizations helped individuals regain confidence in digital platforms.

Participants explained that users were more willing to engage in digital services—such as online banking, health portals, and e-commerce—when they trusted organizations to act ethically and responsibly. These practices fostered digital inclusion, empowering individuals to participate fully in the digital economy without fear of exploitation.

### **Community Level: Building Cyber Awareness and Resilience**

At the community level, participants described how data breach management initiatives fostered awareness, education, and a sense of collective responsibility. Participant 2 discussed cybersecurity outreach programs that “taught community members how to recognize and report scams.” At the same time, Participant 5 emphasized that “shared learning across organizations created a ripple effect that improved cyber hygiene at every level.” Participants 7 and 8 reinforced that transparent communication after cyber incidents encouraged communities to discuss vulnerabilities rather than hide them, thereby normalizing open dialogue about cyber risks.

These practices align with I. Kim et al. (2024), who observed that open communication reduces stigma and motivates victims of data misuse to report incidents. Communities that adopted such open and informed approaches demonstrated greater resilience, as awareness and education replaced fear and uncertainty. Participants agreed that when organizations invested in cybersecurity literacy—through seminars, local training, or public service campaigns—they empowered communities to protect themselves, contributing to a safer digital environment for all.

## **Organizational and Institutional Level: Strengthening Accountability and Governance**

At the organizational and institutional levels, participants underscored that embedding integrated risk management and crisis communication strategies created resilient systems capable of withstanding digital disruptions. Participants 3 and 4 explained that “embedding cybersecurity into governance frameworks” improved accountability, while Participant 9 added that “leadership oversight and ethical reporting practices restored confidence among employees and customers.”

Participants described how aligning cybersecurity protocols with internal control systems, audits, and compliance structures helped build organizational legitimacy and foster a culture of responsibility. Participant 6 emphasized that “transparency in response reporting strengthened institutional credibility, especially in public sector agencies.” These findings supported Ashtiani et al. (2025), who argued that risk-aware governance enhances stability and aligns organizational practices with societal needs for ethical accountability.

Through these measures, institutional leaders demonstrated that effective cybersecurity management was not only a technical mandate but also a public trust obligation. Organizations that embedded data protection within their operational fabric contributed to the broader goal of protecting public interests, ensuring ethical stewardship of information, and aligning with evolving regulatory frameworks such as the Federal Information Security Modernization Act and the General Data Protection Regulation.

### **Societal Level: Advancing Stability, Security, and Public Confidence**

At the societal level, participants acknowledged that data breach management has a direct impact on national security, economic stability, and social trust. Participant 1 emphasized that “data breaches destabilized not only companies but entire sectors,” while Participant 8 added that “a single high-impact breach could undermine public faith in digital governance.” These findings supported Berg et al. (2025), who reported that the ripple effects of data breaches extended beyond single organizations, disrupting markets, eroding trust in institutions, and weakening digital economies.

Participants described how organizations that practiced transparency, collaboration, and ethical accountability contributed to societal resilience. Participant 5 emphasized that “public-private partnerships improved national cybersecurity posture,” while Participant 9 noted that “cross-sector coordination reduced duplication and strengthened collective defense.” These collaborative practices supported economic continuity and enhanced the protection of critical infrastructure across finance, health care, and government sectors. As a result, the study demonstrated that responsible data breach management advanced societal trust in technology. This approach facilitated the development of a more secure digital ecosystem, where innovation, economic growth, and citizen engagement could thrive without undue fear of exploitation or harm.

### **Cultural and Ethical Dimensions: Promoting a Culture of Digital Responsibility**

Across all levels, participants highlighted the ethical and cultural transformation that occurred when organizations treated cybersecurity as a shared responsibility. Participant 2 stated that “cybersecurity culture begins with leadership integrity,” while

Participant 7 emphasized that “ethical accountability defined how organizations regained trust after crises.” These perspectives underscored that cybersecurity had evolved beyond compliance; it had become a cultural value embedded in ethical leadership and organizational behavior.

This cultural shift promoted fairness, transparency, and inclusiveness in digital spaces. As organizations modeled ethical conduct and open communication, employees and consumers internalized these values, creating a ripple effect that strengthened digital citizenship and responsible innovation. These findings confirmed that ethical cybersecurity management served as both a protective mechanism and a catalyst for social progress.

### **Collective Impact and Positive Social Change**

Collectively, these findings revealed that effective data breach management fostered positive social change by enhancing trust, protecting privacy, and promoting institutional legitimacy. The strategies identified, including education, communication, structured response, control integration, and leadership transparency, benefited not only individual organizations but also the broader public sphere.

When organizations prioritized security, transparency, and ethical stewardship, they reinforced public confidence in the digital ecosystem. These actions safeguarded the social contract between individuals and institutions, ensuring that technological advancement remained anchored in accountability and trust. Ultimately, the study’s findings demonstrated that effective cybersecurity management empowered individuals, strengthened communities, and supported stable, equitable, and trustworthy societies.

## **Recommendations for Action**

The findings of this study provided actionable recommendations for business leaders, policymakers, and cybersecurity practitioners seeking to enhance organizational resilience and restore consumer trust following data breaches. The 10 participants confirmed that proactive safeguards, transparent communication, and consumer-centered recovery measures significantly reduced both financial and reputational risks. These recommendations stemmed directly from the study's conclusions and provided specific, actionable steps that organizations could implement to enhance their cybersecurity posture and stakeholder relationships.

### **Recommendation 1: Embed Structured Risk Management Frameworks**

Organizational leaders should integrate structured RMFs into their governance systems to ensure continuous risk identification, assessment, and mitigation. Participants consistently emphasized that the absence of formalized frameworks left organizations vulnerable to recurring breaches and compliance failures. Participant 1 highlighted that “risk management only works when it becomes part of daily operations, not just annual audits.” At the same time, Participant 3 confirmed that “embedding cybersecurity into governance prevented small issues from escalating into crises.”

These perspectives supported CRMT, which emphasized systematic and proactive approaches to managing technological and operational risks. Participants validated that structured risk assessments, adaptive monitoring, and routine evaluations improved their ability to anticipate vulnerabilities and sustain business continuity. Incorporating CRMT principles into enterprise risk frameworks enabled leaders to balance compliance,

financial integrity, and operational resilience. Business executives, chief information security officers, and audit committees should pay particular attention to this recommendation, as it ensures that cybersecurity becomes an integral part of corporate governance rather than a reactive afterthought.

### **Recommendation 2: Operationalize Transparent Crisis Communication Protocols**

Participants emphasized that organizations restored stakeholder confidence more effectively when they implemented transparent and accountable crisis communication protocols. Participant 2 stated that “transparency prevented misinformation from spreading,” and Participant 6 explained that “owning the narrative during a breach restored credibility faster than silence ever could.” These findings align with SCCT, which posits that acknowledging, taking corrective action, and showing empathy can reduce reputational damage during crises (Coombs, 2007). Participants validated this principle through their direct experience, confirming that structured communication—supported by preapproved templates, leadership briefings, and cross-departmental coordination—reduced chaos during breach responses. Business leaders, public affairs officers, and compliance officials should therefore regularly develop and test crisis communication playbooks. These playbooks should define roles, escalation procedures, and message consistency to ensure that both internal staff and external stakeholders receive clear, timely, and honest information during an incident.

### **Recommendation 3: Balance Technical Safeguards with Human-Centered**

#### **Initiatives**

Participants stressed that technological protections remained ineffective without an equally strong human element. Participant 4 emphasized that “firewalls do not fail—people do,” while Participant 8 observed that “training and vigilance filled the gaps that technology alone could not close.” These reflections reinforced that cybersecurity resilience depended as much on culture and behavior as on systems and software.

Organizations should therefore balance technical safeguards such as encryption, multifactor authentication, and artificial intelligence-driven monitoring with ongoing human-centered initiatives. Participants 5 and 9 highlighted that cybersecurity workshops, phishing simulations, and internal awareness campaigns significantly reduced incidents caused by negligence or insider threats. These insights supported Huaman et al. (2022) and Abasi-amefon et al. (2023), who emphasized that combining technical innovation with workforce empowerment cultivated a culture of vigilance and accountability.

Training departments, human resource leaders, and cybersecurity teams should jointly design continuous education programs that align with both compliance requirements and behavioral reinforcement. This dual approach ensured that employees internalized cybersecurity as a personal and organizational responsibility.

### **Recommendation 4: Adopt Consumer-Centered Remediation Measures**

Participants emphasized that post-breach remediation should prioritize consumer welfare and ethical responsibility. Participant 7 stated that “restoring trust meant taking

care of affected consumers first,” while Participant 9 observed that “offering credit monitoring or compensation showed that the organization valued fairness and integrity.”

Participants agreed that consumer-centered recovery measures improved satisfaction, rebuilt loyalty, and reduced litigation risks. These findings supported Hoehle et al. (2022) and Raza et al. (2023), who found that fair and transparent remediation—such as identity protection services or restitution—aligned with consumer expectations and mitigated long-term reputational damage.

Customer service directors, risk officers, and communication teams should jointly design post-breach support programs that include financial monitoring tools, helplines, and transparency portals. These initiatives not only restored individual confidence but also reinforced the organization’s ethical image in the broader marketplace.

#### **Recommendation 5: Institutionalize Continuous Testing and Auditing**

All 10 participants emphasized the importance of regular testing and evaluation in maintaining cybersecurity readiness. Participant 1 explained that “simulation exercises kept the response team sharp,” while Participant 5 noted that “continuous testing revealed unseen weaknesses in both systems and decision chains.”

Organizational leaders should institutionalize regular cybersecurity drills, incident response rehearsals, and independent audits to validate the effectiveness of existing protocols. These practices strengthened both technical and procedural readiness, ensuring that lessons learned from past breaches informed future preventive measures. This proactive approach aligned with CRMT principles by transforming cybersecurity into a cycle of continuous improvement rather than a reactive activity. Chief information

officers (CIOs), compliance managers, and external auditors should collaborate to design and conduct recurring assessments, document and review the findings, and integrate the results into policy revisions.

### **Recommendation 6: Dissemination of Findings and Professional Integration**

The results of this study should be disseminated to both academic and professional audiences to ensure their broad application. Dissemination could occur through several avenues:

- academic dissemination: Submission of scholarly articles to peer-reviewed journals such as the *Journal of Cybersecurity*, *Computers & Security*, and *Journal of Business Research*, focusing on integrating CRMT and SCCT in real-world breach management.
- professional dissemination: presentation of results at industry conferences such as the RSA Conference, Black Hat, Federal Cybersecurity Summit, and Department of Defense Financial Management Symposium, where practitioners can engage with evidence-based strategies.
- organizational training and development: integration of findings into leadership development courses, cybersecurity certification programs, and agency-level workshops across Virginia, Maryland, and Washington, DC.
- policy dissemination: collaboration with policymakers, the Department of Homeland Security, and federal oversight bodies to translate findings into guidelines for public-sector data protection and consumer trust restoration.

These dissemination methods may help ensure that both scholars and practitioners benefit from the study's findings. Dissemination also encourage cross-sector collaboration, advancing the shared goal of creating secure, ethical, and resilient digital infrastructures.

By implementing these recommendations, leaders, policymakers, and practitioners may transform research into actionable policy and operational reform. Embedding CRMT and SCCT principles into governance and communication practices enhanced preparedness, reduced reputational damage, and restored public confidence in digital systems. These findings and recommendations underscore that cybersecurity is not solely a technical obligation but a strategic imperative for sustainable business operations and social responsibility. Disseminating these results through scholarly, professional, and institutional channels may ensure that this research contributes to building a more trustworthy, transparent, and resilient digital society.

### **Recommendations for Further Research**

This study's findings provided meaningful insights into how data managers in Virginia, Maryland, and Washington, DC managed data breaches and restored consumer trust in digital platforms. However, like all qualitative inquiries, this study included limitations that created opportunities for future research. Addressing these limitations would enrich the understanding of cybersecurity risk management and enhance business practices across industries and sectors.

#### **Recommendation 1: Expand the Geographic Scope**

This study focused exclusively on participants located within the Washington, DC metropolitan area, including Virginia and Maryland. While this region represented a

dense hub of financial and governmental institutions, expanding future research to other geographic regions would provide broader insights into how cultural, regulatory, and organizational differences influence breach management strategies. Researchers could compare responses between federal agencies and private corporations across regions such as the West Coast, the Midwest, or international financial centers. Expanding the sample would allow scholars to identify regional variations in cybersecurity resilience, communication approaches, and trust restoration methods, thereby strengthening the generalizability of future findings.

### **Recommendation 2: Increase Sample Size and Diversity**

This study included 10 participants with extensive experience in managing data breaches. Although this number achieved data saturation, future researchers could increase the sample size to capture a broader range of organizational perspectives. Including participants from different hierarchical levels—such as executives, mid-level managers, and technical staff—would deepen understanding of how leadership perspectives align or diverge from operational realities. Future researchers could also explore the experiences of small and medium-sized enterprises (SMEs), nonprofit organizations, and startups, which often face resource constraints that affect their ability to implement robust cybersecurity programs. Expanding participant diversity would enrich the empirical foundation for developing more adaptable and scalable data breach management frameworks.

**Recommendation 3: Conduct Comparative and Quantitative Studies**

I employed a qualitative pragmatic inquiry design to explore strategies for managing data breaches. While qualitative methods revealed in-depth experiences, future researchers could adopt quantitative or mixed methods approaches to measure the effectiveness of specific cybersecurity interventions. For example, future researchers could quantify the correlations between employee training programs and the reduction of breach frequency or evaluate the statistical relationships between communication transparency and consumer trust recovery. A mixed-methods design would combine the depth of qualitative insights with the breadth of quantitative analysis, enabling stronger empirical validation of the relationships identified in this study. Conducting longitudinal studies that track organizational practices over time would also provide valuable evidence on the sustainability of cybersecurity measures and post-breach recovery outcomes.

**Recommendation 4: Explore Consumer and Stakeholder Perspectives**

This study focused primarily on the experiences of data managers who implemented cybersecurity strategies. Future researchers should incorporate the perspectives of consumers, clients, and other stakeholders affected by data breaches. Including these voices could reveal how trust, satisfaction, and loyalty evolved after incidents and how communication strategies influenced perceptions of organizational credibility. Understanding consumer expectations could guide business leaders in developing ethical, transparent, and consumer-centered breach responses. Incorporating this dimension would complement the organizational view of data breach management and promote a more holistic understanding of trust restoration in digital ecosystems.

### **Recommendation 5: Investigate the Role of Artificial Intelligence and Emerging Technologies**

Several participants highlighted the increasing role of AI, automation, and blockchain in preventing and detecting data breaches. Future researchers could explore how these technologies influenced risk management, communication, and trust recovery. Exploring how predictive analytics, AI-driven monitoring, and machine learning applications supported decision-making during crises would expand the theoretical boundaries of CRMT. Researchers could also study how automation affected organizational transparency and ethical decision-making in post-breach communications. Investigating these emerging technologies would offer valuable guidance for organizations seeking to integrate innovation with ethical responsibility.

### **Recommendation 6: Examine Ethical and Psychological Dimensions of Breach Management**

Participants consistently emphasized the emotional and ethical burden that breach management placed on employees and consumers. Future researchers could investigate the psychological effects of cybersecurity crises, including stress, burnout, and moral distress among cybersecurity professionals. Researchers could also analyze how ethical leadership and organizational culture influenced decision-making under crisis conditions. Expanding research into the human and ethical dimensions of breach management would strengthen the link between technical cybersecurity practices and sustainable, values-driven leadership—an essential element of resilient business practice.

**Recommendation 7: Address Identified Methodological Limitations**

The limitations identified in Section 1.12b offered specific areas for methodological refinement. In this study, I relied on self-reported interview data, which may have reflected participants' professional biases or selective recollections. Future researchers could triangulate interview findings with organizational records, incident response documentation, or quantitative performance data to enhance validity and reduce subjectivity. Additionally, this study focused on a single point in time; future longitudinal researchers could examine how strategies evolved as organizations matured in cybersecurity maturity. These methodological improvements would strengthen the dependability and transferability of future studies.

Future researchers should build upon this study's findings to expand theoretical understanding, improve practical applications, and support resilient digital ecosystems. By extending geographic and participant diversity, incorporating quantitative validation, and exploring new technological and ethical dimensions, scholars can deepen insight into how organizations sustain trust and operational stability after cyber incidents. These recommended directions could ensure that future research continues to inform professional practice by providing evidence-based strategies that help business leaders anticipate risks, protect stakeholders, and strengthen cybersecurity governance in an evolving digital world.

**Reflections**

Conducting this doctoral research represented a defining personal and professional milestone that reshaped my perspective on leadership, cybersecurity, and

organizational trust. When I began the study, I brought extensive experience in financial management and internal control, which shaped my understanding of risk and accountability. I initially viewed data breach management as primarily a technical and procedural discipline that required structured systems and compliance oversight. However, as I engaged with the participants and analyzed their experiences, my perspective evolved into a deeper appreciation of the human, cultural, and ethical dimensions that define effective cybersecurity leadership.

### **Researcher Bias and Preconceived Ideas**

At the beginning of the study, I recognized that my professional background could introduce bias. Years of working in structured, policy-driven environments had conditioned me to view cybersecurity mainly through the lens of process efficiency and policy compliance. I acknowledged that this mindset might limit my openness to other perspectives on breach management, particularly those emphasizing communication, trust, and employee engagement.

To mitigate potential bias, I practiced reflexivity throughout the research process. I maintained a reflective journal, recorded decisions made during data collection and analysis, and revisited my assumptions regularly. This discipline helped me remain objective and receptive to participants' insights rather than imposing preconceived frameworks. I also relied on member checking, which allowed participants to confirm that my interpretations accurately represented their experiences. This process reinforced transparency and reduced the influence of personal assumptions.

### **Effects of the Researcher on Participants**

As a professional with subject-matter expertise in risk and data integrity, I understood that participants might perceive me as an evaluator rather than a neutral researcher. To minimize this effect, I created an atmosphere of trust and respect during the interviews. I explained that the study had a scholarly purpose, not a supervisory one. I also assured participants that their experiences would be valued equally, regardless of their roles or industries. By adopting active listening, maintaining an empathetic tone, and encouraging open dialogue, I enabled participants to speak freely about both challenges and successes. Several participants expressed that the interviews offered them an opportunity for self-reflection and professional growth. This reinforced my belief that ethical, human-centered engagement enhanced the authenticity and credibility of qualitative research.

### **Transformation in Thinking**

This study profoundly transformed my understanding of cybersecurity and leadership. Initially, I believed that effective data breach management mainly depended on technology and compliance systems. Through this research, I discovered that trust recovery depended as much on communication, empathy, and organizational culture as on technical proficiency. Participants consistently demonstrated that successful recovery efforts emerged from collaboration, transparency, and ethical leadership. I realized that cybersecurity resilience was not merely about preventing breaches but also about restoring confidence after incidents occurred. This recognition expanded my thinking from focusing on procedural accuracy to emphasizing adaptive leadership, cultural

awareness, and accountability as essential components of digital resilience. The experience taught me that technology alone cannot safeguard organizations without human commitment to integrity, teamwork, and openness. It became clear that leadership effectiveness during crises required a balance of emotional intelligence, communication competence, and technical skill.

### **Scholarly and Professional Growth**

This doctoral journey strengthened my ability to think critically, conduct independent research, and apply academic insights to real-world business challenges. It refined how I synthesized complex data and transformed theoretical concepts into practical strategies. I developed greater awareness of how individual behaviors, leadership styles, and ethical decision-making influence organizational outcomes.

I also learned the importance of patience and persistence, especially in navigating the data collection and analysis process. The challenges I faced—such as aligning interview schedules, organizing large volumes of qualitative data, and maintaining objectivity—enhanced my analytical and problem-solving skills. Most importantly, the process reinforced the importance of humility in scholarship. I recognized that learning continues beyond the completion of a doctoral study, and that effective leadership demands ongoing reflection and adaptability.

Completing this study altered my approach to both scholarship and leadership. I no longer viewed data breach management solely as a technical or operational task but as a broader organizational and social responsibility. The research reminded me that cybersecurity begins and ends with people—their awareness, their actions, and their trust.

As I concluded this journey, I carried forward a renewed sense of purpose as a scholar-practitioner committed to advancing ethical leadership, transparency, and digital trust. This transformation shaped not only my professional practice but also my perspective on how integrity, empathy, and continuous learning form the foundation of effective organizational resilience in the digital age.

### **Conclusion**

After analyzing the data for the study, I concluded that effective data breach management required an integrated approach that combined proactive risk mitigation, transparent crisis communication, and trust-centered recovery. Through the voices of 10 carefully selected participants, the research revealed that organizational preparedness, employee training, and leadership accountability shaped how institutions prevented and responded to digital threats. Each participant described strategies that emphasized education, collaboration, structured response frameworks, embedded controls, and ethical leadership as critical to sustaining consumer confidence in an increasingly interconnected world.

I found that data managers who adopted continuous training programs strengthened both technical readiness and organizational culture. Collaborative communication among cybersecurity teams, system owners, and leadership enabled timely coordination during breach incidents. Structured response protocols—supported by proactive testing and forensics—facilitated swift containment and recovery. Embedding security requirements early in acquisitions and system design proved more effective than implementing reactive safeguards after a breach occurred. Leadership

adaptability also emerged as essential: transformational behaviors fostered long-term resilience, while transactional clarity ensured compliance and focus during times of crisis. Together, these practices reflected a holistic model of digital trust recovery that aligned with both CRMT and SCCT.

The findings reinforced that cybersecurity resilience extends beyond technology; it also depends equally on communication, ethics, and culture. Organizations that integrated CRMT principles—such as proactive risk identification and control implementation—with SCCT’s emphasis on transparency and stakeholder engagement restored trust more effectively and protected reputational integrity. The study demonstrated that preparedness and accountability served as the bridge between technical competence and public confidence.

Professionally, this study contributed to the body of knowledge by translating theory into actionable strategies that business leaders could implement to strengthen digital resilience. The insights provided practical guidance for designing training programs, establishing communication frameworks, and embedding controls into every stage of organizational operations. The findings also supported the idea that data breach management is not a one-time effort but an evolving process that requires constant adaptation, learning, and collaboration. Socially, the study underscored that restoring digital trust benefits not only individual organizations but also the broader community. When institutions safeguard data responsibly and communicate transparently, they reinforce public confidence in digital systems, protect privacy, and contribute to a safer

online environment. These outcomes align with the broader goal of fostering ethical leadership and accountability in an era defined by technological interdependence.

In conclusion, this research provides a comprehensive understanding of how organizations manage cybersecurity risks, restore consumer trust, and maintain operational stability following data breaches. The lessons learned from participants illustrated that effective breach management depends on foresight, collaboration, and integrity in leadership. By integrating human, technological, and strategic elements, organizations built the foundation for enduring trust in the digital economy. Ultimately, this study reaffirmed that ethical, transparent, and resilient leadership remains the cornerstone of sustainable success in the evolving landscape of cybersecurity and digital business management.

## References

- Abasi-amefon, O. A, Nolte, A. & Matulevičius, R. (2023). IoT security risk management: A framework and teaching approach. *Informatics in Education*, 22(4), 555–588.  
<https://doi.org/10.15388/infedu.2023.30>
- Abdullah, M., Ashraf, S., & Noman, A. H. Md. (2025). Cybersecurity risk and corporate greenwashing. *Applied Economics Letters*, 1–7.  
<https://doi.org/10.1080/13504851.2025.2568612>
- Abu, K., Marfo, S., & Ngmenkpieo, F. (2023). Analysis of factors influencing students' choice of business studies in Ghana: Mixed methods research. *Cogent Education*, 10(2), Article 2287913. <https://doi.org/10.1080/2331186X.2023.2287913>
- Ahn, G., Jang, J., Choi, S., & Shin, D. (2024). Research on improving cyber resilience by integrating the zero-trust security model with the MITRE ATT&CK Matrix. *IEEE Access*, 12, 89291–89309. <https://doi.org/10.1109/ACCESS.2024.3417182>
- Akkus, Y., Çetin, B., & Dursunkaya, Z. (2020). A theoretical framework for comprehensive modeling of steadily fed evaporating droplets and the validity of common assumptions. *International Journal of Thermal Sciences*, 158, Article 106529. <https://doi.org/10.1016/j.ijthermalsci.2020.106529>
- Akter, S., Uddin, M. R., Sajib, S., Lee, W. J. T., Michael, K., & Hossain, M. A. (2025). Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. *Annals of Operations Research*, 350(2), 673–698.  
<https://doi.org/10.1007/s10479-022-04844-8>

- Algarni, A. M., Thayanathan, V., & Malaiya, Y. K. (2021). Quantitative assessment of cybersecurity risks for mitigating data breaches in business systems. *Applied Sciences*, *11*(8), Article 3678. <https://doi.org/10.3390/app11083678>
- Alhashmi, S. M., Khedr, A. M., Arif, I., & El Bannany, M. (2021). Using a hybrid-classification method to analyze Twitter data during critical events. *IEEE Access*, *9*, 141023–141035. <https://doi.org/10.1109/ACCESS.2021.3119063>
- Alifia, R.R., Sadeghi, M., Eluru, M., Jafari, M., & Adela Grando, M. A. (2025) Bridging ethical gaps in digital health research: a framework for informed consent aligned with NIH guidance. *BMC Medical Ethics*, *26*, Article 132. <https://doi.org/10.1186/s12910-025-01291-5>
- Allsop, D. B., Chelladurai, J. M., Kimball, E. R., Marks, L. D., & Hendricks, J. J. (2022). Qualitative methods with Nvivo software: A practical guide for analyzing qualitative data. *Psych*, *4*(2), 142-159. <https://doi.org/10.3390/psych4020013>
- Amin, M. E. K., Nørgaard, L. S., Cavaco, A. M., Witry, M. J., Hillman, L., Cernasev, A., & Desselle, S. P. (2020). Establishing trustworthiness and authenticity in qualitative pharmacy research. *Research in Social and Administrative Pharmacy*, *16*(10), 1472–1482. <https://doi.org/10.1016/j.sapharm.2020.02.005>
- Ampel, B. M., Samtani, S., Zhu, H., Chen, H., & Nunamaker, J. F., Jr. (2024). Improving threat mitigation through a cybersecurity risk management framework: A computational design science approach. *Journal of Management Information Systems*, *41*(1), 236–265. <https://doi.org/10.1080/07421222.2023.2301178>

- Antonetti, P., & Baghi, I. (2024). Responding to cyberattacks: the persuasiveness of claiming victimhood. *Journal of Service Research*, 28(3), 434–450.  
<https://doi.org/10.1177/10946705241271337>
- Aruldoss, A., Rana, S., Parayitam, S., & Gurusurthy, B. (2023). Demystifying hedonic shopping motivation and consumer buying behavior during the post-global pandemic: evidence from a developing country. *Journal of Marketing Theory & Practice*, 32(4), 486-505. <https://doi.org/10.1080/10696679.2023.2221442>
- Ashtiani, H. J., Naeiji, S., Zia, A., & Shen, Z. J. (2025). Deep learning-based cybersecurity enhancement strategy in microgrids. *2025 IEEE 34th International Symposium on Industrial Electronics (ISIE)*, 1–6.  
<https://doi.org/10.1109/ISIE62713.2025.11124749>
- Aslam, M., Khan Abbasi, M. A., Khalid, T., Shan, R. U., Ullah, S., Ahmad, T., Saeed, S., Alabbad, D. A., & Ahmad, R. (2022). Getting smarter about smart cities: improving data security and privacy through compliance. *Sensors*, 22(23), Article 9338. <https://doi.org/10.3390/s22239338>
- Bana, S. H., Brynjolfsson, E., Jin, W., Steffen, S., & Wang, X. (2025). Human capital acquisition in response to data breaches. *MIS Quarterly*, 49(1), 367–388.  
<https://doi.org/10.25300/MISQ/2024/18352>
- Berg, J., Holzinger, C., Grüttner, M., & Draxl, A.-K. (2025). Qualitative interview research in multilingual contexts—a comparative discussion of language-related decisions in two empirical studies. *Forum Qualitative Social Research / Forum*

*Qualitative Sozialforschung*, 26(3), Article 15. <https://doi.org/10.17169/fqs-26.3.4367>

Berret, C., & Munzner, T. (2025). Iceberg sensemaking: a process model for critical data analysis. *IEEE Transactions on Visualization and Computer Graphics*, 31(9), 6067–6084. <https://doi.org/10.1109/TVCG.2024.3486613>

Bos, W., & Bunnik, E. M. (2022). Informed consent practices for exome sequencing: an interview study with clinical geneticists in the Netherlands. *Molecular Genetics and Genomic Medicine*, 10(3), Article e1882. <https://doi.org/10.1002/mgg3.1882>

Braun, V., & Clarke, V. (2021). To saturate or not to saturate? Questioning data saturation as a useful concept for thematic analysis and sample-size rationales. *Qualitative Research in Sport, Exercise, and Health*, 13(2), 201-216. <https://doi.org/10.1080/2159676X.2019.1704846>

Calini, C., & Iossa, E. (2024). Multiplicity of tools for antitrust and consumer protection in digital markets: the Italian experience and the road ahead. *European Competition Journal*, 20(2), 274–294. <https://doi.org/10.1080/17441056.2023.2280325>

Chandna, V., & Tiwari, P. (2023). Cybersecurity and the new firm: surviving online threats. *Journal of Business Strategy*, 44(1), 3–12. <https://doi.org/10.1108/JBS-08-2021-0146>

Charura, D. (2020). Psychotherapists' experiences of co-facilitating large encounter PCEP groups: an interpretative phenomenological analysis of six interviews.

*Person-Centered & Experiential Psychotherapies*, 19(3), 251–270.

<https://doi.org/10.1080/14779757.2020.1796770>

Chen, H. S., & Jai, T. M. (2021). Trust fall: data breach perceptions from loyalty and non-loyalty customers. *The Service Industries Journal*, 41(13-14), 947–963.

<https://doi.org/10.1080/02642069.2019.1603296>

Chen, X., Sun, J., & Liu, H. (2022). Balancing web personalization and consumer privacy concerns: mechanisms of consumer trust and reactance. *Journal of Consumer Behavior*, 21(3), 572–582.

<https://doi.org/10.1002/cb.1947>

Cheng, X., Kuang, M., & Yang, H. (2024). Missing data imputation based on causal inference to enhance advanced persistent threat attack prediction. *Symmetry*,

16(11), Article 1551. <https://doi.org/10.3390/sym16111551>

Childress, J. F., & Beauchamp, T. L. (2022). Common morality principles in biomedical ethics: responses to critics. *Cambridge Quarterly of Healthcare Ethics*, 31(2),

164–176. <https://doi.org/10.1017/S0963180121000566>

Coombs, W. T. (2007). Protecting organization reputations during a crisis: the development and application of situation crisis communication theory. *Corporate Reputation Review*, 10(3), 163-176.

<https://doi.org/10.1057/palgrave.crr.1550049>

Cronin, M. A., Stouten, J., & Van Knippenberg, D. (2021). The theory crisis in management research: solving the right problem. *Academy of Management Review*,

46(4), 667–683. <https://doi.org/10.5465/amr.2019.0294>

- Dai, Y., & Wang, T. (2021). Prediction of customer engagement behavior response to marketing posts based on machine learning. *Connection Science*, 33(4), 891–910. <https://doi.org/10.1080/09540091.2021.1912710>
- Daoud, A., & Hamdi, M. (2025). AI and adaptive cybersecurity strategies in higher education institutions (HEIs): towards a secure digital infrastructure. *2025 International Conference On Smart Learning Courses (SCME)*, 120–128. <https://doi.org/10.1109/SCME62582.2025.11104861>
- De Lima, L. A., Ussler, E. R., Bicudo, M. A. S., Menasche, D. S., Kocheturov, A., & Srivastava, G. (2025). Classification of software vulnerability artifacts using public internet data. *2025 IEEE International Conference on Cyber Security and Resilience (CSR)*, 153–158. <https://doi.org/10.1109/CSR64739.2025.11130104>
- Deshpande, S., & Damle, M. (2025). Enhancing IoT security: a pursuit of excellence through the NIST 800-53 cybersecurity framework. *2025 Seventh International Conference on Computational Intelligence and Communication Technologies (CCICT)*, 337–344. <https://doi.org/10.1109/CCICT65753.2025.00060>
- Driggers, K. & Boyles, K. (2024). Epistemology as pragmatic inquiry: rorty, haack, and academic relativism in education. *Studies in Philosophy and Education*, 43, 47–55. <https://doi.org/10.1007/s11217-023-09909-0>
- Durcikova, A., Miranda, S. M., Jensen, M. L., & Wright, R. T. (2024). United we stand, divided we fall: an autogenic perspective on empowering cybersecurity in organizations. *MIS Quarterly*, 48(4), 1503–1536. <https://doi.org/10.25300/misq/2024/17211>

- Egan, C. A., Merica, C. B., Paul, D. R., Bond, L., Rose, S., Martin, A., & Vella, C. (2023). A qualitative evaluation of remote training to develop a fitness surveillance system. *Health Education Journal*, *82*(1), 68–81.  
<https://doi.org/10.1177/00178969221139198>
- Fang, X., Yang, Z., Zhang, Y., & Guo, C. (2023). Adverse effects of data breach on public companies: a study based on interpersonal gossip theory. *Emerging Markets Finance & Trade*, *59*(9), 3094–3107.  
<https://doi.org/10.1080/1540496X.2023.2210721>
- Formentin, M. J., & Coombs, W. T. (2012). Managing corporate social responsibility: A communication approach. *Public Relations Review*, *38*(4), 639–640.  
<https://doi.org/10.1016/j.pubrev.2012.05.011>
- Franke, L., Liang, H., Farzanehpour, S., Brantly, A., Brown, C., & Davis, J. C. (2024). An exploratory mixed-methods study on general data protection regulation (GDPR) compliance in open-source software. *International Symposium on Empirical Software Engineering and Measurement*, 325–336.  
<https://doi.org/10.1145/3674805.3686692>
- Garba, J., Kaur, J., & Nuraihan Mior Ibrahim, E. (2023). Design of a conceptual framework for cybersecurity culture amongst online banking users in Nigeria. *Nigerian Journal of Technology*, *42*(3), 399–405.  
<https://doi.org/10.4314/njt.v42i3.13>

- Garg, P. (2020). Cybersecurity breaches and cash holdings: spillover effect. *Financial Management Association International*, 49(2), 503–519.  
<https://doi.org/10.1111/fima.12274>
- George, M. S., Gaitonde, R., Davey, R., Mohanty, I., & Upton, P. (2023). Engaging participants with research findings: a rights-informed approach. *Health Expectations*, 26(2), 765–773. <https://doi.org/10.1111/hex.13701>
- Haag, S., Siponen, M., & Liu, F. (2021). Protection motivation theory in information systems security research: a review of the past and a road map for the future. *ACM SIGMIS Database: The database for Advances in Information Systems*, 52(2), 25–67. <https://doi.org/10.1145/3462766.3462770>
- Hayden, M., Mattimoe, R., & Jack, L. (2023). The sense of giving role to advisors in farmer decision-making. *Irish Journal of Agricultural and Food Research*, 62(1).  
<https://doi.org/10.15212/ijafr-2023-0105>
- Haughton, N. A. (2023). A pragmatic approach to preparing novice doctoral qualitative researchers. *Journal of the Scholarship of Teaching & Learning*, 23(4).  
<https://doi.org/10.14434/josotl.v23i4.33815>
- He, Y., Xiao, K., Shi, Z., & Zhao, L. (2025). “Dependence” or “critical thinking”? The thinking choices of education doctoral students in a generative AI environment: qualitative research based on interviews. *2025 5th International Conference on Artificial Intelligence and Education (ICAIE)*, 498–503.  
<https://doi.org/10.1109/ICAIE64856.2025.11158573>

- Hennink, M., & Kaiser, B. N. (2022). Sample sizes for saturation in qualitative research: a systematic review of empirical tests. *Social Science & Medicine*, 292. <https://doi.org/10.1016/j.socscimed.2021.114523>
- Hoehle, H., Venkatesh, V., Brown, S. A., Tepper, B. J., & Kude, T. (2022). Impact of customer compensation strategies on outcomes and the mediating role of justice perceptions: a longitudinal study of target's data breach. *MIS Quarterly*, 46(1), 299–340. <https://doi.org/10.25300/MISQ/2022/14740>
- Horton, S., Jackson, V., Boyce, J., Franken, M.-C., Siemers, S., St John, M., Hearps, S., van Reyk, O., Braden, R., Parker, R., Vogel, A. P., Eising, E., Amor, D. J., Irvine, J., Fisher, S. E., Martin, N. G., Reilly, S., Bahlo, M., Scheffer, I., & Morgan, A. (2024). Self-reported stuttering severity is accurate: informing methods for large-scale data collection in stuttering. *Journal of Speech, Language, and Hearing Research*, 67(10S), 4015–4024. [https://doi.org/10.1044/2023\\_JSLHR-23-00081](https://doi.org/10.1044/2023_JSLHR-23-00081)
- Huaman, C. H. O., Fuster, N. F., Luyo, A. C., & Armas-Aguirre, J. (2022). Critical data security model: gap security identification and risk analysis in the financial Sector. *2022 17th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–6. <https://doi.org/10.23919/CISTI54924.2022.9820547>
- Humaidi, N., & Shahrom, M. (2023). Assessing employees' cybersecurity attitude based on working and cybersecurity threat experience. *The African Journal of Information Systems*, 15(3), Article 3. <https://digitalcommons.kennesaw.edu/ajis/vol15/iss3/3/>

- Husband, G. (2020). Ethical data collection and recognizing the impact of semistructured interviews on research respondents. *Education Sciences*, 10(8), Article 206.  
<https://doi.org/10.3390/educsci10080206>
- Iglesias, G., Talavera, E., González-Prieto, Á., Mozo, A., & Gómez-Canaval, S. (2023). Data augmentation techniques in the time series domain: A survey and taxonomy. *Neural Computing & Applications*, 35, 10123–10145.  
<https://doi.org/10.1007/s00521-023-08459-3>
- Janvrin, D. J., & Wang, T. (2022). Linking cybersecurity and accounting: an event, impact, response framework. *Accounting Horizons*, 36(4), 67–112.  
<https://doi.org/10.2308/HORIZONS-2020-101>
- Jarjoui, S., Murimi, R. (2021). A framework for enterprise cybersecurity risk management. in: Daimi, K., People, C. (eds) advances in cybersecurity management. *Springer, Cham*. [https://doi.org/10.1007/978-3-030-71381-2\\_8](https://doi.org/10.1007/978-3-030-71381-2_8)
- Jeremy, J., & Spandagou, I. (2025). Shadowing as qualitative inquiry: exploring its potential and limitations in educational research. *International Journal of Qualitative Methods*, 24. <https://doi.org/10.1177/16094069251330720>
- Kamariotou, M. & Fotis Kitsios. (2023). Information systems strategy and security policy: a conceptual framework. *Electronics*, 12(2), Article 382.  
<https://doi.org/10.3390/electronics12020382>
- Kamenjarska, T., Josimovski, S., & Pulevska Ivanovska, L. (2020). Ethical decision-making and game theory applications for cyber security in the insurance markets:

A survey. *Journal of Sustainable Development (1857-8519)*, 10(25), 30–41.

<https://www.ceeol.com/search/article-detail?id=920251>

Kane, M. (2023). Edelman barometer reveals trust and credibility are suffering. *Vision Monday*. <https://www.visionmonday.com/vm-events/vm-summit/article/edelman-barometer-reveals-trust-and-credibility-are-suffering/>

Kelly, L. M., & Cordeiro, M. (2020). Three principles of pragmatism for research on organizational processes. *Methodological Innovations*, 13(2).

<https://doi.org/10.1177/2059799120937242>

Khan, S., Kabanov, I., Hua, Y., & Madnick, S. (2022). A systematic analysis of the capital one data breach: critical lessons learned. *ACM Transactions on Privacy & Security*, 26(1), Article 3. <https://doi.org/10.1145/3546068>

Kim, L. (2021). Cybersecurity and related challenges during the COVID-19 pandemic. *Nursing*, 51(2), 17–20. <https://doi.org/10.1097/01.NURSE.0000731916.83045.e6>

Kim, I., Jang, J., Shin, D., Park, M., Lee, H.-J., & Lee, S. (2024). A study on the multi-cyber range application of mission-based cybersecurity testing and evaluation in association with the risk management framework. *Information*, 15(1).

<https://doi.org/10.3390/info15010018>

Kim, I., Kim, S., Kim, H., & Shin, D. (2022). Mission-based cybersecurity test and evaluation of weapon systems in association with risk management framework.

*Symmetry*, 14(11), Article 2361. <https://doi.org/10.3390/sym14112361>

Kochetkov, E. P. (2024). The impact of the digital technological revolution on the development of crisis management theory. *MIR (Modernization Innovation*

*Research*), 15(2), 298–314. <https://doi.org/10.18184/2079-4665.2024.15.2.298-314>

Koh, J., Caron, S., Watters, A. N., Vaidyanathan, M., Melnick, D., Santi, A., Hudson, K., Arguelles, C., Mathur, P., & Etemadi, M. (2025). Technological adjuncts to streamline patient recruitment, informed consent, and data management processes in clinical research: observational study. *JMIR Formative Research*, 9, Article e58628. <https://doi.org/10.2196/58628>

Kolevski, D., Michael, K., & Freeman, M. (2025). In this special issue: data breaches in the cloud—business security and risk management. *IEEE transactions on technology and society, technology and society*, 6(1), 2–14. <https://doi.org/10.1109/TTS.2024.3477828>

Kumar, T., Alwaisi, Z., Gupta, A. K., Auluck, N., & Mohonen, P. (2025). Analyzing sustainable security for 6g networks. *2025 IEEE conference on communications and network security (CNS)*, 1–7. <https://doi.org/10.1109/CNS66487.2025.11194975>

Kure, H. I., Islam, S., Ghazanfar, M., Raza, A., & Pasha, M. (2022). Asset criticality and risk prediction for an effective cybersecurity risk management of the cyber-physical system. *Neural Computing & Applications*, 34, 493–514. <https://doi.org/10.1007/s00521-021-06400-0>

Labrecque, L. I., Markos, E., Swani, K., & Peña, P. (2021). When data security goes wrong: examining the impact of stress, social contract violation, and data type on

- consumer coping responses following a data breach. *Journal of Business Research*, 135, 559–571. <https://doi.org/10.1016/j.jbusres.2021.06.054>
- Linneberg, M., & Korsgaard, S. (2019). Coding qualitative data: a synthesis guiding the novice. *Qualitative Research Journal*, 19(3), 259–270. <https://doi.org/10.1108/QRJ-12-2018-0012>
- Liu, L. Y. (2025). Financial statement audits and data breaches. *Management Science*, 71(8), 6340–6366. <https://doi.org/10.1287/mnsc.2023.01357>
- Lopopolo, O., Bienati, A., Frey, J.-C., Glaznieks, A., & Spina, S. (2025). Categorizing speakers' language background: theoretical assumptions and methodological challenges for learner corpus research. *Research Methods in Applied Linguistics*, 4(1). <https://doi.org/10.1016/j.rmal.2024.100170>
- Mahuwi, L., & Israel, B. (2024). Promoting transparency and accountability towards anti-corruption in the pharmaceutical procurement system: does e-procurement play a significant role? *Management Matters*, 21(1), 20–37. <https://doi.org/10.1108/MANM-07-2023-0027>
- Malatji, M. (2024). Evaluating human-machine interaction paradigms for effective human-artificial intelligence collaboration in cybersecurity. *2024 International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA)*, 1268–1272. <https://doi.org/10.1109/ICICYTA64807.2024.10913015>
- Mann, Z. A. (2024). Urgency in cybersecurity risk management: toward a solid theory. *2024 IEEE 37th Computer Security Foundations Symposium (CSF)*, 651–664. <https://doi.org/10.1109/CSF61375.2024.00051>

- Mawel, M., & Sambasivam, S. (2023). Exploring the strategic cybersecurity defense information technology managers should implement to reduce healthcare data breaches. *Information Systems Education Journal*, 21(3), 4–11.  
<https://files.eric.ed.gov/fulltext/EJ1392669.pdf>
- Maxwell, J. A. (2022). Interactive approaches to qualitative research design. *Interactive Approach to Qualitative Research Design*, 2, 41–54.  
<https://doi.org/10.4135/9781529770278.n4>
- Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity enterprises' policies: a comparative study. *Sensors*, 22(2), Article 538.  
<https://doi.org/10.3390/s22020538>
- Mitroff, I. I. (1994). Crisis management and environmentalism: a natural fit. *California Management Review*, 36(2), 101–113. <https://doi.org/10.2307/41165747>
- Moernaut, N. (2021). Listening between the lines: how a theoretical framework prevents superficial analysis in qualitative research. *New Trends in Qualitative Research*, 6, 15–23. <https://doi.org/10.36367/ntqr.6.2021.15-23>
- Mora-Navarro, G., Femenia-Ribera, C., Velilla Torres, J. M., & Martinez-Llario, J. (2022). Geographical data and metadata on land administration in Spain. *Land*, 11(7), Article 1107. <https://doi.org/10.3390/land11071107>
- Morgan, M. D., Chowdhury, M. M., & Latif, S. (2021). Protecting business from data breach. *2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, 1–5.  
<https://doi.org/10.1109/ICECCME52200.2021.9590975>

Morrow, R. L., Mintzes, B., Gray, G., Law, M. R., Garrison, S., & Dormuth, C. R.

(2023). Public reporting of clinical trial findings as an ethical responsibility to participants: a qualitative study. *BMJ Open*, *13*(3), Article e068221.

<https://doi.org/10.1136/bmjopen-2022-068221>

Motulsky, S. L. (2021). Is member checking the gold standard of quality in qualitative research? *Qualitative Psychology*, *8*(3), 389–406.

<https://doi.org/10.1037/qup0000215>

Naeem, M., Ozuem, W., Howell, K., & Ranfagni, S. (2024). Demystification and actualization of data saturation in qualitative research through thematic analysis.

*International Journal of Qualitative Methods*, *23*.

<https://doi.org/10.1177/16094069241229777>

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*. Department of Health, Education, and Welfare. <https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html>

National Institute of Standards and Technology. (2018, December). *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy* (Special Publication No. 800-37, Rev. 2). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.SP.800-37r2>

- Nie, C., Li, J., & Wang, S. (2020). Modeling the effect of spending on cyber security by using surplus process. *Mathematical Problems in Engineering*, 2020(1), 1–10. <https://doi.org/10.1155/2020/3239591>
- Nikkhah, H. R., & Grover, V. (2024). Strategizing responses to data breaches: a multi-method study of organizational responsibility and effective communication with stakeholders. *Journal of Management Information Systems*, 41(4), 1042–1077. <https://doi.org/10.1080/07421222.2024.2415774>
- Ohneberg, C., Warmbein, A., Stöbich, N., Rathgeber, I., Kruppa, A., Nast-Kolb, J., Träger, M. F., Bahou, A., Stahl, O., Eberl, I., & Fischer, U. (2022). Study protocol for the implementation and evaluation of a digital-robotic-based intervention for nurses and patients in a hospital: a quantitative and qualitative triangulation based on the Medical Research Council (MRC) framework for developing and evaluating complex interventions. *BMC Nursing*, 21, Article 349. <https://doi.org/10.1186/s12912-022-01088-6>
- Olmos-Vega, F. M., Stalmeijer, R. E., Varpio, L., & Kahlke, R. (2023). A practical guide to reflexivity in qualitative research: AMEE guide no. 149. *Medical Teacher*, 45(3), 241–251. <https://doi.org/10.1080/0142159X.2022.2057287>
- Ozarpa, C., Avci, I., & Khan, Y. Z. (2025). Ethics and security in the digital world: recommendations for cybersecurity strategies and practices in Türkiye. *2025 9th International Symposium on Innovative Approaches in Smart Technologies (ISAS)*, 1–9. <https://doi.org/10.1109/ISAS66241.2025.11101777>

- Pang, M.-S., & Vance, A. (2025). Breached and denied: the cost of data breaches on individuals as mortgage application denials. *MIS Quarterly*, 49(2), 465–494. <https://doi.org/10.25300/misq/2024/18787>
- Parsons, N. R., Basu, J., & Stallard, N. (2024). Group sequential designs for pragmatic clinical trials with early outcomes: methods and guidance for planning and implementation. *BMC Medical Research Methodology*, 24, Article 42. <https://doi.org/10.1186/s12874-024-02174-w>
- Pearson, H., Myall, M., Darlington, A.-S., & Gibson, F. (2025). The approach and application of analyzing inductive and deductive datasets: a worked example using reflexive thematic analysis. *Qualitative Research in Psychology*, 22(4), 842–886. <https://doi.org/10.1080/14780887.2025.2499265>
- Peel, K. L. (2020). A beginner’s guide to applied educational research using thematic analysis. *Practical Assessment, Research & Evaluation*, 25(2), 1–15. <https://doi.org/10.7275/ryr5-k983>
- Pratt, M. G. (2025). On the evolution of qualitative methods in organizational research. *Annual Review of Organizational Psychology and Organizational Behavior*, 12, 109–131. <https://doi.org/10.1146/annurev-orgpsych-111722-032953>
- Qazi, M.S. (2023). Applying situational crisis communication theory (SCCT) to crisis termination dynamics in south Asia: an assessment of actor roles and responses. *Journal of Security & Strategic Analyses*, 9(2), 23–39. <https://doi.org/10.57169/jssa.009.02.0254>

- Rahman, M. D., Quadri, G. J., Doppalapudi, B., Szafir, D. A., & Rosen, P. (2024). A qualitative analysis of common practices in annotations: a taxonomy and design space. *IEEE Transactions on Visualization and Computer Graphics*, 31(1), 360–370. <https://doi.org/10.1109/TVCG.2024.3456359>
- Raza, B., St-Onge, S., & Ali, M. (2023). Frontline employees' performance in the financial services industry: the significance of trust, empathy, and consumer orientation. *International Journal of Bank Marketing*, 41(3), 527–549. <https://doi.org/10.1108/IJBM-06-2022-0237>
- 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>
- Rivera, J. D. (2023). Cultural competency for emergency and crisis management: Concepts, theories and case studies. *Public Administration Review*, 83(4), 994–996. <https://doi.org/10.1111/puar.13680>
- Rosati, P., Gogolin, F., & Lynn, T. (2022). Cyber-security incidents and audit quality. *European Accounting Review*, 31(3), 701–728. <https://doi.org/10.1080/09638180.2020.1856162>
- Rose, J., & Johnson, C. W. (2020). Contextualizing reliability and validity in qualitative research: toward more rigorous and trustworthy qualitative social science in leisure research. *Journal of Leisure Research*, 51(4), 432–451. <https://doi.org/10.1080/00222216.2020.1722042>

- Rouse, E., Reinecke, J., Ravasi, D., Langley, A., Grimes, M., & Gruber, M. (2025). From the editors: making a theoretical contribution with qualitative research. *Academy of Management Journal*, 68(2), 257–266. <https://doi.org/10.5465/amj.2025.4002>
- Sato, A., Okazaki, A., Yoshida, K., & Iizuka, K. (2022). The influence of instagram on cosmetic buying behavior. *2022 12th International Congress on Advanced Applied Informatics (IIAI-AAI)*, 529–534. <https://doi.org/10.1109/IIAIAAI55812.2022.00108>
- Schneier, B., & Vance, A. (2025). “Complexity is the worst enemy of security”: studying cybersecurity through the lens of organizational complexity. *MIS Quarterly*, 49(1), 205–210. <https://doi.org/10.25300/misq/2025/49.1.075>
- Seyedi, S., Jiang, Z., Rad, A. B., Clifford, G. D., Griner, E., Iacobelli, L., Cotes, R. O., Corbin, L., Roberts, K., Milloy, A., Boazak, M., & Abbasi, A. (2023). Using HIPAA (health insurance portability and accountability act)–compliant transcription services for virtual psychiatric interviews: pilot comparison study. *JMIR Mental Health*, 10, Article e48517. <https://doi.org/10.2196/48517>
- Shah, P. K., Shah, A. V., & Pandya, H. B. (2025). A Comprehensive Review of IoT Network Security using Machine Learning Techniques. *2025 International Conference on Modern Sustainable Systems (CMSS)*, 1105–1111. <https://doi.org/10.1109/CMSS66566.2025.11182403>
- Sharma, P., Tiwari, S., Choi, T., & Kaul, A. (2024). Big data analytics for crisis management from an information processing theory perspective: A

multimethodological study. *IEEE Transactions on Engineering Management*, 71, 10585–10599. <https://doi.org/10.1109/TEM.2022.3209786>

Silas, G. S., & Rajsingh, E. B. (2024). A pragmatic inquiry to learn recent trends in insider threat detection approaches. *2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT)*, 1918–1923.

<https://doi.org/10.1109/ICCPCT61902.2024.10672670>

Smith, R. W., Chandler, J. J., & Schwarz, N. (2020). Uniformity: the effects of organizational attire on judgments and attributes. *Journal of Applied Social Psychology*, 50(5), 299–312. <https://doi.org/10.1111/jasp.12660>

Smits, D., Beusekom, B. V., Martin, F., Veen, L., Geleijnse, G., & Moncada-Torres, A. (2022). An improved infrastructure for privacy-preserving analysis of patient data. *Studies in Health Technology & Informatics*, 295, 144–147.

<https://doi.org/10.3233/SHTI220682>

Sorn, J., Carroll, P., Pang, Z., Bhunia, S., Salman, M., & Regis, P. A. (2024). Exploring the cam4 data breach: security vulnerabilities and response strategies. *2024 IEEE 24th International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, 174–179.

<https://doi.org/10.1109/CCGridW63211.2024.00028>

Spanca, F., & Salihu, A. (2024). Unveiling the consequences of data breaches: risks, impacts, and mitigation in the digital age. *2024 International Conference on Electrical, Communication and Computer Engineering (ICECCE)*, 1–8.

<https://doi.org/10.1109/ICECCE63537.2024.10823432>

- Tewelde, A. I. (2023). 'The merged researcher' and 'emergent subjectivity': complicating reflexivity in migration research. *International Journal of Sociology*, 53(3), 228–238. <https://doi.org/10.1080/00207659.2023.2200620>
- Tingare, B. A., Prasanna Lakshmi, G., Khedkar, V., Suresh Babu, R. T., Dhar Diwan, T., & Khatkale, P. B. (2024). Responsible AI on the national cybersecurity strategy with the enhancement of cybersecurity in education. *2024 International Conference on Intelligent & Innovative Practices in Engineering & Management (IIPEM)*, 1–6. <https://doi.org/10.1109/IIPEM62726.2024.10925807>
- Toombs, E., Skov, B., Campbell, M., Lund, J., & Mushquash, C. J. (2025). A scoping review of indigenous community-based research practices, guidelines, and ethical standards. *Canadian Journal of Public Health*. <https://doi.org/10.17269/s41997-025-01090-w>
- Uddin, M. R., Akter, S., & Lee, W. J. T. (2024). Developing a data breach protection capability framework in retailing. *International Journal of Production Economics*, 271. <https://doi.org/10.1016/j.ijpe.2024.109202>
- Ullah, B., & Nabii, S. I. (2022). Developing cyber security strategies for business organizations to prevent data breaches. *KASBIT Business Journal*, 15(4), 62-79. <https://research.ebsco.com/c/riljaj/viewer/html/gbe7svs6pr>
- Valdez, C. R., Brabeck, K. M., Barajas-Gonzalez, R. G., Ayón, C., & Rojas-Flores, L. (2024). Socio-politically and trauma-informed public health practice with latino families: conceptual framework and best practices. *American Journal of Public Health*, 114(S6), S485–S494. <https://doi.org/10.2105/AJPH.2024.307589>

- Valencia, J., Alie, S., Wulandari, R., & Hamali, S. (2024). Effect of security, privacy, and customer satisfaction on e-commerce consumer trust. *2024 International Conference on Informatics, Multimedia, Cyber and Information Systems (ICIMCIS)*, 429–434. <https://doi.org/10.1109/ICIMCIS63449.2024.10957101>
- Venketesh, K., Gunalan, M. C., R, M. H., S, R., & R, S. (2025). Anti-remote disk imaging: a comprehensive approach to prevent unauthorized data access. *2025 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI)*, 1–6. <https://doi.org/10.1109/ICDSAAI65575.2025.11011811>
- Vivek, Y. Nanthagopan, & S. Piriyaatharshan. (2023). Beyond methodology: theoretical foundations of triangulation in qualitative and multi-method research: a literature review. *Scientific Studies on Social and Political Psychology*, 29(2), 53–62. <https://doi.org/10.61727/ssspj/2.2023.53>
- Wellberg, S., & Evans, C. (2022). Assumptions underlying performance assessment reforms intended to improve instructional practices: a research-based framework. *Practical Assessment, Research & Evaluation*, 27, Article 23. <https://doi.org/10.7275/pare.1334>
- Weyant, E. (2022). Research design: qualitative, quantitative, and mixed methods approaches, 5th edition. *Journal of Electronic Resources in Medical Libraries*, 19(1-2), 54–55. <https://doi.org/10.1080/15424065.2022.2046231>
- Yang, N., Korfiatis, N., Zisis, D., & Spanaki, K. (2024). Incorporating topic membership in review rating prediction from unstructured data: a gradient boosting approach.

*Annals of Operations Research*, 339, 631–662. <https://doi.org/10.1007/s10479-023-05336-z>

- Yin, R. K. (2018). Case study research and applications: design and methods (6th ed.). SAGE Publications. <https://us.sagepub.com/en-us/nam/case-study-research-and-applications/book250150>
- Zhang, J. Z., Goel, L., & Williamson, S. (2024). Understanding enterprise cybersecurity information sharing: a theoretical model and empirical analysis. *Enterprise Information Systems*, 18(3). <https://doi.org/10.1080/17517575.2024.2310844>
- Zhang, H., Peng, J., Mao, J., & Xu, S. (2025). Repeated data breaches and executive compensation. *Applied Economics Letters*, 32(8), 1111–1120. <https://doi.org/10.1080/13504851.2024.2302552>
- Zhu, Q., Duan, Y., & Sarkis, J. (2024). Supply chain carbon transparency to consumers via blockchain: does the truth hurt? *The International Journal of Logistics Management*, 35(3), 833–864. <https://doi.org/10.1108/IJLM-03-2023-0109>
- Zhu, J. J., Tuo, L., You, Y., Fei, Q., & Thomson, M. (2024). A preemptive and curative solution to mitigate data breaches: corporate social responsibility as a double layer of protection. *Journal of Marketing Research (JMR)*, 61(4), 778–801. <https://doi.org/10.1177/00222437231218969>
- Zhu, M., & Wang, J. (2025). Exploration and practice of data thinking in the application of e-commerce art design course under the background of big data. *Expert Systems*, 42(1), Article e13493. <https://doi.org/10.1111/exsy.13493>

## Appendix: Interview Protocol

### **Primary Business Research Phenomenon Under Study and Overarching Research**

#### **Question**

The topic of research is "Digital Trust Recovery: Effective Data Breach Management Approaches." The overarching research question is: What strategies do data managers in Virginia, Maryland, and DC use to manage data breaches and restore consumer trust in digital platforms?

#### **Primary Research Goal**

The purpose of this interview is to explore strategies data managers employ to mitigate the effects of data breaches, restore consumer trust, and sustain organizational operations.

#### **Introduction**

1. Thank you for agreeing to participate in this research study. Your insights are vital in understanding effective data breach management strategies and their impact on consumer trust.
2. I will conduct interviews with several data managers to gather comprehensive information for this study. Before proceeding, I would like to review a few key details.
3. Participation in this study is entirely voluntary. You may decline to answer any question or withdraw at any time without any penalty.
4. With your permission, I will audio-record this interview to ensure accuracy. After transcription, I will review the data to maintain the integrity of your responses.

5. Your identity and organization will remain confidential. Pseudonyms will be used in reports and publications to protect privacy.
6. All data will be securely stored for five years and then destroyed in accordance with ethical research practices.
7. Do you have any questions or concerns before we begin?
8. This interview is expected to take 60–90 minutes. Is this timeframe acceptable for you?
9. Are you comfortable proceeding with audio recording?
10. Let us begin.

#### **Initial Probe Questions**

1. Please state your name and title.
2. What is your current role and scope of responsibility regarding data management and cybersecurity?
3. How would you describe your tenure and experience in handling data breaches?

#### **Targeted Interview Questions**

1. What specific strategies have you implemented to manage data breaches?
2. Can you outline the steps involved in executing these strategies effectively?
3. What significant challenges have you faced in managing data breaches, and how have you addressed them?
4. How do you evaluate the success of your data breach management strategies?
5. What impact has effective breach management had on restoring consumer trust in your organization?

6. Could you share examples where these strategies significantly affected consumer trust?
7. How do you align your data management strategies with emerging cybersecurity threats?
8. In your view, what trends or challenges will shape data breach management in the near future?

### **Follow-Up Questions**

1. Why are specific organizational resources critical in managing data breaches effectively?
2. How do your strategies address both immediate and long-term impacts of data breaches?
3. Why do you measure strategic success in the manner described?

### **Closing**

1. Thank you for your valuable insights and time. Your contributions are crucial for this study.
2. I may schedule a follow-up session to review the transcript for accuracy. Would a tentative date be acceptable to you?
3. Please feel free to reach out if you have any additional thoughts or questions after this interview.
4. Again, thank you for participating. Your input is highly appreciated.