

12-30-2025

Information Technology Managers' Strategies for Securing Organizational Networks From Cyberattacks

Damilola O. Jibowu
Walden University

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

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

Walden University

College of Management and Human Potential

This is to certify that the doctoral study by

Damilola O. Jibowu

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. Constance Blanson, Committee Chairperson, Information Technology Faculty
Dr. Gary Griffith, Committee Member, Information Technology Faculty

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

Walden University
2025

Abstract

Information Technology Managers' Strategies for Securing Organizational Networks

From Cyberattacks

by

Damilola O. Jibowu

MBA, Abubakar Tafawa Balewa University, Nigeria, 2009

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

February 2026

Abstract

Cyberattacks increasingly threaten enterprise networks, creating significant risks to sensitive data and business operations. The purpose of this qualitative pragmatic inquiry was to explore the strategies Information Technology (IT) managers use to secure organizational networks from cyberattacks. Participants consisted of seven experienced IT managers with a minimum of 5 years of network security management experience, purposefully selected through LinkedIn. The study was grounded in integrated systems theory, which emphasizes the interdependence of technology, processes, and risk management within organizations. Data were collected through semistructured interviews and document analysis to examine practical approaches to securing networks. Thematic analysis identified eight core strategies: conducting regular risk assessments and mitigation, enforcing governance and compliance standards, building layered security architectures, strengthening user training and awareness, leveraging threat intelligence for adaptive defense, developing proactive incident response capabilities, securing operational technology environments, and aligning practices with government standards and Zero Trust principles. Based on these findings, the study recommends that organizations implement a comprehensive cybersecurity framework that integrates these strategies to reduce the likelihood of successful cyberattacks and enhance overall enterprise resilience. The implications for positive social change include the potential for IT managers and business leaders to implement integrated cybersecurity strategies that reduce data breaches, strengthen digital trust, and promote safer organizational and community environments.

Information Technology Managers' Strategies for Securing Organizational Networks

From Cyberattacks

by

Damilola O. Jibowu

MBA, Abubakar Tafawa Balewa University, Nigeria, 2009

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

February 2026

Dedication

This work is dedicated, first and foremost, to the loving memory of my parents: my beloved father, Olufunmi Oladipo Jibowu, the Ogboye of Ijeun, and my beloved mother, Victoria Olabisi Aroba. Your love and sacrifices laid the foundation of my life's journey, your memory remains a pillar of strength and inspiration, and I carry both your gentle spirits in all I do.

And to the remarkable memory of my grandfather, Sir Olumuyiwa Jibowu, a trailblazing Nigerian jurist who broke barriers as the first African to serve on the Supreme Court of Nigeria, the first African police magistrate, the first Nigerian High Court judge, a pioneer of the Nigerian judiciary, and one-time Chief Justice of the Western Region. Your legacy of excellence and service to humanity ignites a fire in me. I am inspired to make a difference in the lives of others as you did.

To my second mother, Debra Windapo, thank you for your steadfast love, support, and prayers. Your presence in my life has been a blessing beyond measure.

To my incredible children, Tise and Tami, may this accomplishment be a reminder that with faith, discipline, and dedication, no dream is too far to reach. You are my joy, my motivation, and my future. To all my sisters and brothers, I hope this stands as a motivation and inspiration for you to know that your dreams are achievable.

To my cherished wife, Mercy Temitope Jibowu, the rock behind me, your patience, love, and encouragement have been the backbone of this journey. I am grateful for your unwavering belief in me. This dissertation stands as a tribute to all of you, my roots, my support, and my inspiration. Above all, I dedicate this to you, babe, we did it!!

Acknowledgments

First and foremost, I extend my deepest gratitude and sincere appreciation to my committee chair, Dr. Constance Blanson. Your insightful guidance, unwavering support, and steadfast encouragement throughout my doctoral journey have been pivotal to my success. Your commitment to excellence, coupled with your remarkable ability to inspire and challenge me, has significantly enhanced the depth and quality of my research. I am forever grateful for your mentorship, Dr. B, you rock!

I would also like to express profound appreciation to my second committee member, Dr. Gary Griffith. Your constructive feedback, meticulous attention to detail, and thoughtful suggestions have enriched my dissertation immeasurably. Your expertise and dedication have been invaluable in helping me refine and elevate my scholarly work.

Special thanks go to the program coordinator, Dr. Miles, and the distinguished faculty members who have contributed significantly to my academic and professional growth during this journey: Dr. Jodine Burchell, Dr. Donald Carpenter, Dr. Robert Duhainy, Dr. Lawrence Fulton, Dr. Andy Igonor, Dr. Nawaz Khan, Dr. Patrick Mensah, Dr. Jon McKeeby, Dr. Cynthia Phillips, Dr. Shaun A. Sullivan, Dr. Don Carpenter, Dr. Dana Haywood, and Dr. Cheryl Waters. Your collective wisdom, support, and encouragement have broadened my perspectives and profoundly impacted my learning experience.

Table of Contents

List of Tables	v
Section 1: Foundation of the Study.....	1
Background of the Problem	1
Information Technology Problem Focus and Project Purpose	1
Research Question	3
Assumptions and Limitations	3
Assumptions.....	3
Limitations	4
Significance of the Study	5
Contribution to Information Technology Practice.....	6
To the Practitioners.....	6
To the Practice	6
Implications for Social Change.....	7
Transition and Summary.....	8
Section 2: Literature Review	10
Literature Review Summary.....	10
Organization of the Literature Review	12
A Review of the Professional and Academic Literature.....	13
Integrated Systems Theory	15
Risk Management in Network Security.....	17
Internal Controls in Network Security.....	17

Cyberattacks in Network Security	18
Synthesis	20
Gaps in the Literature.....	21
Strategies for Strengthening Cybersecurity Defenses.....	21
Integration of Risk Management and Internal Controls	23
Internal Controls for Network Security	24
Innovative Strategies Leveraging AI and Emerging Technologies	25
Internal Control—The Human Factor.....	26
Mitigating Human Vulnerabilities in Network Security.....	27
Evaluating Network Security Effectiveness in Risk Management	28
Adapting to Emerging Threats Through Risk Management.....	29
Integrated Cybersecurity Strategies: Technology, People, and Compliance	29
Barriers to Implementing Effective Network Security	30
Collaboration and Decision-Making in Network Security	31
Improvements in Network Security	31
Secure Networks From Cyberattacks.....	32
Research With Similar and Differing Research Results	34
Transition and Summary.....	35
Section 3: The Project.....	37
Project Ethics	37
Nature of the Project	39
Population, Sampling, and Participants	40

Data Collection Activities.....	41
Interview Questions	44
Data Organization and Analysis Technique	45
Reliability and Validity.....	47
Transferability.....	48
Credibility	48
Confirmability.....	49
Transition and Summary.....	50
Section 4: Application to Professional Practice and Implications for Change	51
Introduction.....	51
Overview of the Study	51
Presentation of the Findings.....	52
Internal Control Table.....	52
Risk Management and Thematic Analysis Tables.....	54
Thematic Summary.....	56
Findings and Thematic Focus	60
First Theme: Risk Assessment & Mitigation.....	61
Second Theme: Security Governance & Compliance Enforcement.....	70
Third Theme: Comprehensive Security Architecture	77
Fourth Theme: User Security Training & Awareness	82
Fifth Theme: Threat Intelligence & Adaptive Defense	87
Sixth Theme: Cyberattack Defense & Incident Management	92

Seventh Theme: Operational Technology & Industrial Security.....	98
Eighth Theme: Government Cybersecurity Standards & Zero Trust	103
Security Framework Adoption Across Themes.....	108
IT Contributions and Recommendations for Professional Practice.....	111
IT Leaders: Practical Applications of Findings	111
Actionable Recommendations for IT Leaders	111
Message to the Research-Scholar Community	114
Implications for Social Change.....	116
Recommendations for Further Research.....	118
Conclusion	120
References.....	123
Appendix A: Interview Questions	138
Appendix B: Glossary of Terms	139
Appendix C: Interview Protocol	144

List of Tables

Table 1. Internal Security Control Comparison.....	53
Table 2. Risk Management Strategy Comparison	55
Table 3. Thematic Summary.....	58
Table 4. Subthemes in Risk Assessment & Mitigation Theme	62
Table 5. Subthemes in Security Governance & Compliance Enforcement Theme.....	70
Table 6. Subthemes in Comprehensive Security Architecture Theme	77
Table 7. Subthemes in User Security Training & Awareness Theme	82
Table 8. Subthemes in Threat Intelligence & Adaptive Defense Theme	87
Table 9. Subthemes in Cyberattack Defense & Incident Management Theme	93
Table 10 Subthemes in Operational Technology & Industrial Security Theme.....	98
Table 11. Subthemes in Government Cybersecurity Standards & Zero Trust Theme ...	103
Table 12. Security Framework Adoption.....	110

Section 1: Foundation of the Study

Background of the Problem

Data breaches and cybersecurity threats have become an inevitable reality in today's digital landscape, with cyberattacks occurring frequently across industries globally. As businesses increasingly rely on interconnected networks and digital infrastructure, their systems have become more vulnerable, exposing them to a variety of sophisticated cyberattacks (Aslan et al., 2023). The effects of these attacks are typically disastrous, from operational halts to very damaging reputational losses, and they may even hinder the business for a long time (Rodrigues et al., 2024). Quickly changing technology has increased these challenges, making it impossible for organizations to maintain a secure network. For instance, sectors such as agriculture, healthcare, and energy experienced an over 50% increase in ransomware attacks in 2024. The healthcare sector alone had a 128% increase in the United States and an almost twofold increase globally, reflecting the increasing exposure for industries that manage sensitive information (Office of the Director of National Intelligence, 2024). According to Kioskli et al. (2023), up to 95% of cybersecurity breaches are due to human factors, highlighting the need for approaches that reach beyond the technical deterrents of security with models for human behavior such as those represented by adaptive approaches such as Zero Trust (Sarkar et al., 2022).

Information Technology Problem Focus and Project Purpose

The vulnerability loopholes in the defense of enterprise networks expose organizational operations and sensitive information to preeminent risks (Afolalu &

Tsoeu, 2025). The number and severity of data breaches have increased significantly in recent years, especially ransomware attacks affecting industries like financial services and real estate (National University, 2024). These trends reflect the growing prevalence of sophisticated cyberattacks such as unauthorized access, malware, and phishing. The general information technology (IT) problem is that some IT managers lack effective strategies for securing their organizations' networks. The specific IT problem is that some IT managers lack strategies for securing their organizations' networks from cyberattacks, leaving them vulnerable to a wide range of cyber threats.

The purpose of this qualitative pragmatic inquiry study was to explore strategies used by IT managers to secure their organizations networks against cyberattacks. The study focused on IT managers within enterprise organizations. A purposeful sampling method was employed to select six to seven participants who met the eligibility criteria. Invitations to participate were sent through LinkedIn.

Data were collected through semistructured interviews and document analysis. These methods enabled an in-depth exploration of the strategies IT managers use to integrate risk management and internal controls into their cybersecurity practices, addressing critical gaps in network security. This study contributes to the understanding of how IT managers can better secure networks from cyberattacks and inform organizational efforts to enhance cybersecurity defenses.

The study is grounded in an integrated systems theory (IST) for information security management (ISM), developed by Hong et al. (2003). This framework synthesizes concepts from security policy theory, risk management, control and auditing,

management systems, and contingency theory, emphasizing the interconnectedness of technology, processes, and risk management strategies within organizations. Although this theory is domain-specific to ISM, it covers critical components such as risk management, internal control measures, security policies, auditing, and contingency planning, all of which directly align with the research focus on how IT managers integrate risk management and internal controls to secure networks from vulnerability attacks. With the findings, I aim to provide actionable insights for improving organizational security postures, reducing the risk of cyberattacks, and strengthening overall network resilience (Hong et al., 2003).

By identifying effective strategies, this study has the potential to drive positive social change by fostering a safer digital environment. Organizations equipped with robust cybersecurity practices can reduce the risks of data breaches, identity theft, and privacy violations, thereby supporting a more secure digital economy and building greater trust in digital interactions (Domnik & Holland, 2024).

Research Question

What effective strategies do IT managers use to secure networks from cybersecurity attacks?

Assumptions and Limitations

Assumptions

Assumptions are preliminary beliefs accepted as true without empirical verification, forming the basis upon which research is conducted (Belina, 2022).

According to Belina (2022), assumptions are considered facts that the researcher accepts

but cannot directly verify. In qualitative research, assumptions help define the scope of the study and guide methodological decisions, even though they do not guarantee certainty (Taquette & Borges da Matta Souza, 2022). This study operated under several key assumptions. It was assumed that the IT managers participating in this study had a genuine interest in contributing to the research and participated openly in interviews to enhance their understanding of network security strategies. Secondly, it was supposed that the participants complied with their statements concerning their cybersecurity activities, that is, as regards their cultivating risk and control through risk management internal controls. It was assumed that the perceptions from the interviews in this study reflected what is being practiced more than would have been the case if these were theoretical or idealistic applications, and the participants' perceptions were regarded as an accurate reflection of the current tactics used in network security practice. Finally, it was assumed that the overall security landscape and cybersecurity issues relevant to IT managers would continue to be of a similar nature throughout the research project, ensuring that the findings remained applicable and relevant throughout the research.

Limitations

Limitations are barriers or obstacles that circumscribe a study and that are likely to affect the meaning or generalisability of the research findings (Busse et al., 2016). There are some caveats, however. First, it might be hard to have access to an adequate number of IT managers, since security practices are of a confidential nature and participants might not wish to disclose in-depth information. A further limitation is that it may be difficult to get specific information about how IT managers incorporate risk

management and internal controls (since this information may be proprietary and participants may be unlikely to reveal it). Also, it is an ethical limitation, since obtaining and verifying informed consent, keeping confidentiality, and honoring the voluntary participation of the individuals are very important in all research work.

Another limitation affecting this study was money to produce interview guides and get into databases, which could have limited the breadth of the study. An additional limitation was the risk of response bias, whereby participants might have provided answers they perceived as favorable or expected rather than their actual practices. Moreover, the rapid evolution of cybersecurity technologies posed a limitation, as changes in the field during the study could have affected participants' perspectives and the relevance of the findings. Finally, the study's geographic focus on IT managers may have limited the generalizability of the findings to other industries, potentially reducing the applicability of the results to broader contexts.

Significance of the Study

The contribution of this study was to solve important problems in network security, and to provide a basis for IT practitioners, enterprises, and society. With cyber threats advancing, there is mounting pressure on companies to guard their networks with strong security. This qualitative research provides IT practitioners with successful strategies for improving their organizational cybersecurity. This study provides critical contributions to society, including the field of IT, as it addresses the need for implementing successful strategies to secure organizational networks.

Contribution to Information Technology Practice

To the Practitioners

This study is also relevant to practitioners and IT professionals responsible for protecting enterprise networks from emerging threats. As a result of the increasing dependence of organizations on network communication, businesses have to cope with the challenge of protecting sensitive information and maintaining operations while heavy cyberattacks are launched on these interlinked computer systems (Barraza de la Paz et al., 2023). The implications of the results are actionable such that they show how to actually include risk management and internal control in cybersecurity. This information is vital for IT managers, who need to modify their strategies based on new menaces and ensure that their security is in line with industry standards. In addition, businesses using these learnings can limit their exposure to cyber risks, lower their likelihood of suffering data breaches, and maintain the trust of their customers and wider stakeholder community (Rodrigues et al., 2024). By concentrating on real-world tactics that link theory to practice, this research could help IT practitioners strengthen their security architecture and maintain security from online threats.

To the Practice

The purpose of this research was to contribute significantly to IT practice by giving insight into the usage of risk management and internal control measures in the context of network security. Cybersecurity is less about technology alone and more about a disciplined and holistic approach, including strategic planning, vigilant monitoring, and incorporating the human element such as user behavior and insider risk (Sarkar et al.,

2022). Previous studies did not provide a clear understanding of how IT managers can incorporate these practices into their organisations' cybersecurity strategies, which created a gap in knowledge that this study aimed to address. This approach is essential to tackle human error, a common factor that results in as much as 95% of security breaches (Mishra et al., 2022). The findings from this work offer practical guidance to IT managers on adopting more proactive and resilient cybersecurity practices, ensuring that their approaches remain effective in a constantly evolving threat landscape. This research also informs policy development by helping IT leaders identify where to invest in cybersecurity measures that will deliver the greatest impact.

Implications for Social Change

This study may serve as an agent for social change by improving the capability of IT managers to protect their networks from cyberattacks, resulting in a safer and more reliable online environment. By minimizing the incidence and damage caused by data breaches, this research contributes to shielding people's sensitive personal and financial data and lowers the chances of identity theft, financial loss, and privacy infringements.

According to Aslan et al. (2023), the ever-changing face of cyber risks, combined with their escalating complexity, underlines the necessity for novel approaches to the management of this kind of threat. In facing these challenges, the results of this study provide actionable information for IT managers to defend critical infrastructure and help create a safer digital world.

Additionally, through fostering a tone of accountability, transparency, and active security practices, this research supports the creation of a culture of ethical cybersecurity

management in congruence with social norms of responsibility and equity. In turn, this may create a more resilient digital ecosystem that empowers individuals, strengthens communities, and supports the ongoing development of inclusive, secure, and trustworthy digital societies.

Transition and Summary

Section 1 provided a comprehensive overview of the study, including the background of the problem, the problem statement, and the purpose of exploring strategies for securing organizational networks against cyberattacks. This section outlined the research methodology and design, emphasizing the use of a qualitative pragmatic inquiry approach. It also explained the theoretical background, assumptions, limitations, and implications of the study, including the implications for positive social change, by providing practical applications toward meaning for IT practitioners and IT practice. A review of the professional and academic literature was also performed in order to frame the problems and the existing holes of the network security context, giving the base for the study. In Section 2, I restate the purpose statement and delve into a detailed review of the relevant literature, offering a comprehensive analysis of the existing research on cybersecurity strategies, risk management, and internal controls. I discuss the theoretical frame of reference and the themes that were used to guide the research study. Section 3 presents the study design, including the role of the researcher, description of participants, methods of data collection, process of data analysis, and strategies to establish data trustworthiness. Finally, in Section 4, I outline the study's results and findings, examining the practical and theoretical implications in relation to professional practice and focus on

social change. It is filled with advice from IT leaders who were looking to boost their cybersecurity defenses and protect their networks.

Section 2: Literature Review

Literature Review Summary

The aim of this literature review is to analyze the best practices IT managers should undertake to secure and prevent their organization's networks against new cybersecurity challenges. The need to adapt to more sophisticated cyber threats has led to the development of a holistic approach, blending technical, organizational, and human-centered approaches. This overview leveraged published peer-reviewed articles, government reports, and seminal books to present a clear picture on the current state of network security.

Risk management and internal controls have been identified as pivotal components of effective cybersecurity practices. Studies highlight that technical measures, such as encryption, firewalls, and intrusion detection systems, form the first line of defense Ambreen et al. (2024). However, Ferreira et al. (2023) emphasize the need to integrate these tools with organizational practices, including regular compliance audits and security awareness training. Such integration has been shown to mitigate over 85% of common vulnerabilities, yet challenges persist in adapting these strategies to evolving work environments, particularly with the rise of remote and hybrid work models (Alghamdi, 2022).

Emerging technologies, such as artificial intelligence (AI) and Zero Trust Architecture, are increasingly recognized as transformative tools for combating sophisticated cyberattacks. AI-driven threat detection has shown promise in identifying anomalies and mitigating advanced persistent threats (Phiayura & Teerakanok, 2023).

Nevertheless, Macas et al. (2022) caution that integrating AI with legacy systems and ensuring scalability for small to medium-sized enterprises remain significant obstacles. Zero Trust Architecture, which mandates continuous verification of user identity and device integrity, has similarly faced resistance due to its complexity and high implementation costs (Y. Zhang, 2023).

Human error, accounting for over 90% of cybersecurity breaches, remains a persistent challenge despite advances in technology (Melaku, 2023). Employee training, access management protocols, and robust internal controls are critical for reducing risks associated with misconfigurations and negligence. The alignment of human-centered strategies with technical controls is essential for building a resilient cybersecurity framework, as it addresses both organizational and technological challenges. However, as highlighted in recent government reports, the lack of consistent enforcement of such practices continues to leave organizations vulnerable to insider threats (Hinsz & Nickell, 2024).

This literature review underscores the breadth of inquiry into cybersecurity strategies by examining both technical and non-technical solutions. The synthesis of diverse sources demonstrates the necessity of adopting a holistic approach that combines innovative technologies, organizational processes, and human-centered strategies to effectively address network vulnerabilities. These findings provide a robust foundation for understanding and addressing the persistent cybersecurity gaps faced by organizations and highlight critical opportunities for future research to enhance network resilience in the face of evolving threats.

Organization of the Literature Review

This study reviewed the related literature on the integration of risk management, internal controls, and network security strategies in an organized manner by considering such key concepts. The structure of the review consists of five main sections in order to ensure a smooth reading and full comprehension of the topic.

Theoretical foundations: Firstly, this paper looks into an IST for ISM developed by Hong et al. (2003). This theory highlights the interplay between technical, organizational, and human components in the resolution of information security issues, and it provides the conceptual framework of this research.

Second, the review moves on to risk management approaches, examining how firms practice the process of discovering, evaluating, and managing risks. This subsection discusses proactive measures, which include technical solutions such as firewalls and encryption, in addition to organizational processes such as compliance audits and monitoring systems (Liu et al., 2021).

Third, the discussion focuses on internal controls in terms of access controls, audits, and compliance measures that help secure network defenses. This part discusses the importance of human error as a primary cause of security breaches, as well as the necessity of educating and sensitizing employees continuously to reduce risks (Mishra et al., 2022).

Fourth, the review explores future directions in security, including emerging technologies and artificial intelligence-driven solutions, along with Zero Trust Architecture, that may provide avenues for improving the security of the enterprise. This

section also addresses the challenges of integrating artificial intelligence solutions with legacy systems and concerns about scalability for smaller organizations (Akhtar & Rawol, 2024).

The review concludes by discussing how the main themes, theoretical foundation, risk framework, internal control, human factor, and artificial intelligence-based solutions, relate to the research problem and are synthesized. The thrust of this synthesis is to discover how IT managers combine those strategies in order to successfully address the vulnerabilities of their network. This systematic review allows for a comprehensive examination of the literature, thus providing a solid basis for identifying critical gaps and generating actionable recommendations in the field of network security.

A Review of the Professional and Academic Literature

A literature review is about reviewing, synthesizing, and commenting on the literature that already exists to develop new knowledge, idea, and/or awakening on a topic (Rana et al., 2023). I categorized the literature elements based on existing scholarships. For example, Salkind (2010) and Cooper (1988) categorize these elements into focus, goals, perspective, organization, method of synthesis, coverage, and audience, while Torraco (2016) groups them into three categories: literature review, research methods, and theories. In the literature review, key sources were synthesized, to include the exploration of current knowledge, relevant theories, research methods, gaps, and a critique of the literature to generate new insights.

A strategic search of various comprehensive databases, including ProQuest, IEEE Xplore, Google Scholar, JSTOR, and the Walden University Library, peer-reviewed

journal articles, dissertations, and reports related to cybersecurity were used. Key search terms such as "Cybersecurity strategies," "IT managers," "Risk management in cybersecurity," "Internal controls," "Network Security," "Cyberattacks," and "Cybersecurity in the U.S." were used to refine the results. Boolean operators (AND, OR) were used to combine terms, such as "cybersecurity strategies AND IT managers."

An iterative search process, starting with broad terms like "cybersecurity strategies" and "network security" was used to build a general understanding of the topic. Then, the focus was narrowed by using more specific terms, such as "cyberattacks" and "risk management integration." This allowed a deeper exploration on how IT managers address vulnerability gaps. When limited results on region-specific strategies were encountered, the search was expanded to include conference proceedings, white papers, and dissertations, helping to capture and identify emerging trends. For instance, searches like "internal controls + Network breaches" provided niche insights.

In areas where current research was scarce, older foundational studies were referenced to fill gaps, providing the necessary historical context and theoretical grounding. A full list of search terms and combinations is included within Appendix B, which details the iterative process used to ensure comprehensive coverage of the topic.

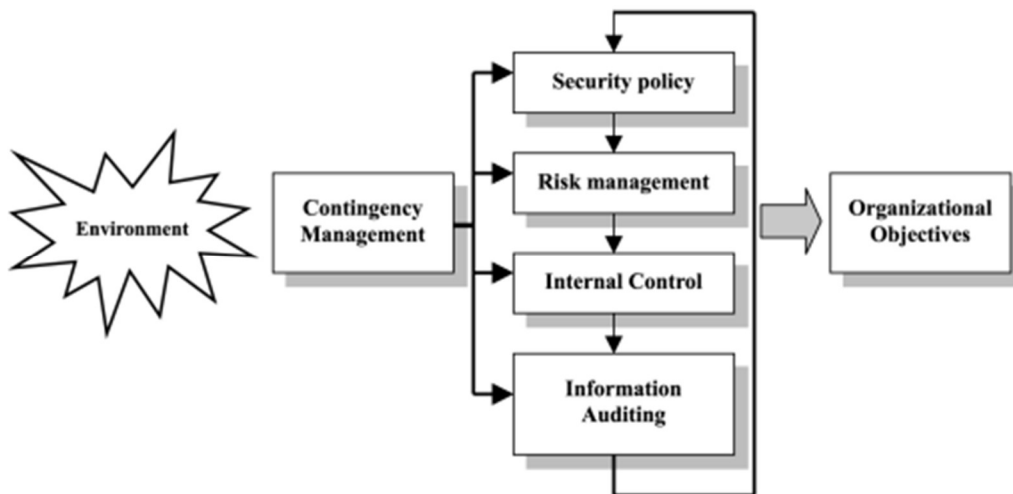
The purpose of the study was to examine successful practices of IT managers in embedding risk management and internal controls in order to protect the organization's networks from cyberattacks. The work is built upon IST, which explains how technical, organizational, and human components are interconnected within cybersecurity systems.

The literature review aimed to explore previous research on risk management and internal controls within the field of network security, especially in the context of cyberattacks. It also examined how IST has been applied to cybersecurity strategies and emerging technologies, including artificial intelligence-based solutions. Through this review, the study identified gaps in existing knowledge, particularly the lack of a unified approach that effectively blends technical defenses with human-centered processes. Addressing these gaps, the current study provides insights into how IT managers can design comprehensive and flexible strategies to strengthen network resilience against evolving cyber threats.

Integrated Systems Theory

Figure 1

Integrated Systems Theory



Note. Reprinted from Hong, S., Kim, H., & Lee, C. (2003). *An integrated systems theory for information security management (ISM)*. *Information Management & Computer Security*, 11(5), 243–248. Used under fair use for academic purposes.

An IST for ISM, developed by Hong et al. (2003), provides a comprehensive framework for understanding how different parts of an organization work together to support security. The theory highlights that technical infrastructure, internal policies, risk management strategies, internal controls, and security procedures are all interdependent. A weakness in any one area can compromise the entire system. This holistic view is especially important in cybersecurity, where both technology and human behavior must align to create an effective defense system.

IST and Network Security

In the context of network security, IST explains how IT managers incorporate risk management and internal control mechanisms to address cybersecurity threats. The theory emphasizes the importance of coordination between technical measures and human behavior to achieve effective protection. Risk management involves identifying, assessing, and addressing potential threats, while internal controls such as access restrictions and audits help ensure ongoing system security. Research by Mishra et al. (2022) points out that human error remains one of the leading causes of security breaches, and that regular training and awareness programs are critical for reducing these vulnerabilities.

Primary Writings and Key Theorists

Hong et al. (2003) presented an IST for ISM, suggesting that organizations should be viewed as unified systems where a failure in one component can put the entire structure at risk. Kritzing and von Solms (2010) applied this idea to cybersecurity for home users, showing that a combination of technical tools and human-focused strategies

can significantly reduce security incidents. Building on this, Barraza de la Paz et al. (2023) highlighted that effective risk management in cybersecurity involves balancing technical solutions like encryption with broader organizational practices such as auditing and compliance.

Application of IST in Previous Research

IST has been used to address a variety of cybersecurity problems. Kritzinger and von Solms (2010) employed it as a means to raise awareness in home users about cybersecurity, while Barraza de la Paz et al. (2023) discussed the role of public-private partnership in cybersecurity risk mitigation. De Nobrega et al. (2024) extended the theory to cyberattacks, making arguments about combining technical defenses with organizational practices. They argued that, cyberattacks should not be treated as standalone events, but instead as indicators of deeper systemic flaws in an organization

Risk Management in Network Security

Effective risk management is critical for identifying, evaluating, and mitigating threats to organizational networks.

Internal Controls in Network Security

Ambika and Sujatha (2024) mention how IT managers need to move past technical implementations and focus on vigilant monitoring and strong policy enforcement to effectively reduce human-related vulnerabilities. Chang et al. (2021) highlights the importance of compliance-related internal controls in reducing financial misstatements, noting that deficiencies in compliance controls strongly correlate with organizational risks. Similarly, Cheong et al. (2021) emphasize the critical role of

control-related disclosures in mitigating reputational and operational risks, further demonstrating the significance of internal controls as part of a comprehensive risk management framework. Litt et al. (2023) extend this discussion by illustrating how the absence of robust internal controls, as evidenced by cybersecurity breaches, can damage organizational reputation and erode trust among stakeholders.

IST's framework advocates for the integration of internal controls with risk management practices to form a unified approach to security. By combining human-centered internal controls with technology-based defenses, IT managers can create more resilient networks. This study aims to explore how IT managers implement both risk management and internal control strategies to secure their networks from cyberattacks.

Cyberattacks in Network Security

Modern cyberattacks reveal critical vulnerabilities in both technical systems and human behaviors within organizations, making a holistic and integrated approach essential for effective defense. Mishra et al. (2022) explain that cyberattacks are rarely isolated incidents. Instead, they tend to exploit multiple vulnerabilities across an organization's infrastructure, highlighting the importance of a well-coordinated security response. Traditional security measures often fail to keep up with these complex threats, which can take advantage of outdated software, unpatched systems, and poorly trained users. IST offers a helpful framework for managing these risks by emphasizing the connections between technical systems, organizational processes, and human behavior. Cassottana et al. (2023) support this approach, encouraging IT managers to develop strategies that combine technical safeguards with human-centered initiatives.

By treating cybersecurity as a system of interrelated components, IST allows organizations to address the root causes of vulnerabilities instead of just managing the symptoms. This kind of approach not only strengthens technical defenses but also promotes ongoing employee training and organizational awareness programs. The result is a more comprehensive and resilient security posture. To protect against modern cyberattacks, organizations need solutions that integrate both technical tools and human elements.

Kioskli et al. (2023) research results demonstrates the need for IT managers to lessen their dependability on automated security functions. A systems-based approach under IST supports ongoing auditing, vulnerability assessments, and employee education as part of a complete cybersecurity strategy. Ayodele and Buttigieg (2024) highlight the value of innovative technologies like software-defined networking, which helps improve network defenses by allowing scalable, automated responses to new threats. This is especially beneficial for organizations facing economic or resource constraints that limit their ability to frequently update software or offer extensive training.

By focusing on critical vulnerabilities and implementing scalable solutions, organizations can build stronger defenses without overspending. Badrinath et al. (2023) and Chen et al. (2023) both support this cost-effective approach. Ultimately, IST encourages a flexible and resilient security framework that blends risk management with human-centered strategies, providing a strong foundation to protect against the constantly evolving landscape of cyber threats.

Synthesis

The literature review makes it evident that the network security issues faced by IT managers are multidimensional and should be addressed in a holistic way. The integrated framework for ISM proposed by Hong et al. (2003) provides a solid grounding in how technical, organizational, and human elements need to come together to create comprehensive and effective security.

Risk management and internal controls are two critical foundations for establishing cybersecurity strategy. Risk management is the process of identifying, assessing, and responding to risks, while internal controls are needed to ensure that protections are in place, such as access restrictions and compliance procedures, to avoid security breaches (Ambika & Sujatha, 2024). These two controls help prevent known vulnerabilities and reduce human errors, which are often the cause of security breaches (Mishra et al., 2022). From the perspective of integrated systems, it is essential to treat all these components as connected. Neither risk management nor internal controls are effective in isolation. They should be incorporated into a larger structure that includes continuous supervision, employee education, and strict adherence to security policies (Khodadadyan et al., 2021).

As IT managers are often working under financial or organizational constraints, this integrated approach is especially relevant. By using IST, they can develop broader strategies to tackle threats from multiple directions, including technical systems, organizational structures, and human behavior (Kritzinger & von Solms, 2010). This

approach provides a flexible and resilient foundation for cybersecurity that can adapt to evolving digital threats.

Gaps in the Literature

The present study aims to address this gap by examining how IT managers apply principles from IST, including risk management and internal controls, to protect their networks from cyberattacks. This research seeks to offer a clearer understanding of how these strategies are applied in practice, with the goal of helping organizations strengthen their cybersecurity posture, lower their exposure to cyber threats, and enhance overall network resilience. The findings from this study will have the potential to foster positive social change by contributing to a safer digital environment. As organizations become more effective at protecting sensitive data, the risk of data breaches, identity theft, and privacy violations may be reduced. This, in turn, supports greater trust in digital interactions and contributes to a more secure digital economy.

Strategies for Strengthening Cybersecurity Defenses

The literature on cybersecurity highlights various strategies for addressing organizational challenges, with a particular focus on strengthening network resilience, mitigating vulnerability risks, and improving security awareness. Aksoy (2024) emphasize the transformative potential of AI-driven cybersecurity training to bridge education and implementation gaps by offering tailored solutions that adapt to evolving risks and regulatory demands. This focus on individualized education contrasts with Kaur and Ramkumar (2022), who address systemic and policy-level cybersecurity challenges, highlighting the importance of national strategies and workforce development to secure

critical infrastructure. Both studies, however, converge on the importance of education and awareness as foundational strategies for enhancing cybersecurity. In terms of risk management, Cremer et al. (2024) draw attention to significant gaps in cyber insurance policies, emphasizing how exclusions poorly align with realized risks. This analysis provides a counterpoint to the proactive defense frameworks proposed by Monteiro et al. (2023), who advocate for mission-oriented security strategies that integrate cyber-physical measures to enhance resilience against cascading failures. Together, these studies underline the need for a multifaceted approach to risk management that combines policy alignment with proactive and strategic defenses.

Gautam (2023) contributed to the discussion on strengthening cybersecurity defenses by exploring how deep reinforcement learning (DRL) can be leveraged to enhance system resilience against evolving cyber threats. By applying DRL within complex networked infrastructures, such as power and energy systems, the study illustrated the potential of intelligent, adaptive technologies to detect, respond to, and recover from sophisticated attacks. This reinforces the strategic value of integrating AI-driven solutions into cybersecurity frameworks to proactively manage emerging technical challenges, which aligns with Akhtar and Rawol (2024) emphasis on proactive measures but extends the focus to include cutting-edge technical solutions. These studies collectively provide a comprehensive view of the strategies required to address the general problem of IT managers lacking strategies for securing their organizations networks from cyberattacks. They underscore the need for integrated approaches that combine education, policy reforms, strategic defenses, and advanced technologies. This

synthesis directly informs the research question, “What strategies do IT managers use to secure their organizations networks from cyberattacks?” by offering critical frameworks and evidence-based solutions for improving network security and resilience.

Integration of Risk Management and Internal Controls

The integration of risk management and internal controls is a foundational strategy for cybersecurity resilience in complex organizational environments.

Khodadadyan et al. (2021) asserted that, effective risk management requires the combined application of human expertise and technological tools, especially in highly regulated sectors. Human judgment plays a critical role in evaluating threats that automated systems might miss. Asasfeh et al. (2024) reinforced this position, noting that insider threats in complex systems often evade detection by technical tools and require nuanced human interpretation. These studies highlight the importance of aligning internal controls with organizational governance, emphasizing that risk mitigation should be embedded into decision-making processes and not treated as an isolated function.

Adding to this discourse, Rikhardsson et al. (2021) argued that, risk management in high-pressure environments such as banking must be responsive and collaborative, incorporating insights from both top management and IT auditors. Khelil and Khlif (2022) echoed this sentiment, highlighting that auditors in the public sector perceive their role as more effective when integrated into the broader internal control and risk assessment framework. However, smaller organizations face barriers due to limited resources, a challenge noted by Akhtar and Rawol (2024), who suggested that, integrating artificial intelligence (AI) and machine learning (ML) into threat detection

may help overcome such constraints. Together, these findings indicated that successful integration requires a balance of strategic leadership, intelligent automation, and scalable implementation to foster adaptive, proactive cybersecurity environments.

Internal Controls for Network Security

Internal controls are critical for maintaining the integrity of network security systems, particularly in a threat landscape characterized by increasingly sophisticated attacks. Ahmadi (2024) underscored the importance of Zero Trust Architecture (ZTA) in modern control strategies. ZTA enforces strict identity verification and network segmentation, thereby limiting lateral movement within a system, even if a perimeter is breached. J. Zhang et al. (2022) advanced this notion by emphasizing hybrid isolation models within ZTA environments, particularly sandboxing, to contain malicious code and preserve operational continuity.

In industrial contexts, Chen et al. (2023) highlighted the effectiveness of Role-Based Access Control (RBAC) in managing access within multi-domain systems. RBAC supports the principle of least privilege, allowing only authorized users to interact with critical infrastructure, thus reducing the likelihood of unauthorized access. Y. Zhang (2023) took this a step further by illustrating how hybrid computational intelligence systems can strengthen ZTA implementations by combining privacy preservation with real-time anomaly detection, especially useful in sensitive environments such as educational or healthcare systems.

Kim et al. (2023) and Aksoy (2024) argued that the successful implementation of internal control strategies like ZTA and RBAC depends not only on technological

sophistication but also on organizational culture and leadership. Their studies indicated that without strong management support and a cybersecurity-aware culture, even the most advanced controls may fail to achieve their intended impact. This suggests that internal controls must be both technically robust and culturally embedded to be truly effective.

Innovative Strategies Leveraging AI and Emerging Technologies

The reviewed literature underscores innovative strategies IT managers can adopt to secure organizational networks against cyberattacks, aligning with the general problem of lacking effective cybersecurity strategies. At the heart of these studies is the use of artificial intelligence, machine learning, and other advanced technologies to strengthen network security. Artificial intelligence-powered intrusion detection systems have shown significant promise, especially with models like federated learning that offer decentralized protection while maintaining data privacy (Olanrewaju-George & Pranggono, 2025). Explainable artificial intelligence adds further value to malware detection by making the decision-making process more transparent and trustworthy, helping IT managers make better-informed security decisions (Baghirov, 2025).

In response to the growing threat of cyberattacks, researchers have explored scalable authentication and access control frameworks for Internet of Things devices, highlighting practical solutions for securing endpoints in environments with limited resources (Kokila & Reddy, 2025; Magara & Zhou, 2025). Handling missing data in intrusion detection datasets has also emerged as a key strategy, improving data quality and the accuracy of anomaly detection systems (Tahir et al., 2025).

In addition, cybersecurity for Industry 4.0 systems, particularly in the manufacturing sector, emphasizes the importance of cybersecurity training and awareness among IT managers (Alqudhaibi et al., 2025). These insights directly contribute to the research question by outlining actionable strategies for IT managers, including better data management, the integration of artificial intelligence technologies, and the promotion of cybersecurity awareness across the organization.

Internal Control—The Human Factor

Human factors are critical in network security, particularly when it comes to managing risks caused by human error, such as incorrect system configurations. Security training and awareness programs play a key role in reducing these risks. Khodadadyan et al. (2021) and Asasfeh et al. (2024) highlight the value of human expertise in complementing automated tools. While automated systems are useful, they lack the nuanced judgment that people bring to decision-making, especially in environments governed by strict regulations. A secure network depends on the effective integration of both human and technological components.

However, human error remains one of the main causes of network vulnerabilities, with configuration mistakes being a common issue. Kioskli et al. (2023) and Asasfeh et al. (2024) point out that such misconfigurations are often the result of poor cyber hygiene and a lack of employee awareness. Their research shows that focused, human-centered training and continuous staff education are essential to reduce these types of risks.

Training plays a central role in helping employees understand how to avoid and fix potential vulnerabilities before they can be exploited. Taherdoost (2024) emphasizes

the importance of running cybersecurity awareness programs, especially during times of disruption. These programs not only improve technical knowledge but also help reinforce the consequences of mistakes and ensure staff follow security protocols.

In environments like remote work and cloud-based systems, training becomes even more important. Mugwagwa et al. (2024) found that in these settings, proper training helps prevent data loss and misconfigurations, both of which are common security weaknesses. Organizations can also learn from past incidents. For example, the SolarWinds breach showed how failures in internal processes could be exploited. Marelli (2022) explained that using lessons from such breaches can help improve employee training and reduce repeated mistakes.

Although human expertise adds significant value to automated security tools, the ongoing risk of human error, especially misconfigurations, makes continuous and comprehensive training a necessary part of any strong cybersecurity strategy. Khelil and Khlif (2022) added that internal auditors are crucial in detecting and correcting errors, ensuring that internal controls are functioning as intended. To secure vulnerabilities, IT managers must integrate human expertise, regular training, and awareness programs to maintain a strong security posture.

Mitigating Human Vulnerabilities in Network Security

The integration of human-centric strategies and technological advancements is critical for addressing contemporary cybersecurity challenges comprehensively. Research highlights the importance of tailoring interventions to address human factors, such as cognitive biases and behavioral intentions, which often act as entry points for

cyberattacks (Aschwanden et al., 2024). Tailored behavioral strategies, particularly in SMEs, have been shown to significantly reduce cybersecurity risks compared to generic approaches. Motivation is also a critical factor in cybersecurity. Hinsz and Nickell (2024) introduced an integrated model that encourages secure cybersecurity behaviors, drawing on concepts like the theory of planned behavior. Their research identified behavioral intentions as strong predictors of secure actions, shaped by individual attitudes, social expectations, and a person's sense of control over their actions.

On the technology side, advancements such as software-defined wide area network architectures offer powerful solutions for today's cybersecurity needs, as explored by Johnson and Patel (2024). These technologies boost network resilience but still face challenges, particularly in working smoothly with older legacy systems.

Taken together, these studies highlight the importance of connecting both human and technological strategies. A combined approach is essential for building strong network defenses against cyberattacks. Ongoing challenges like scaling solutions and overcoming resistance to change show why continued research and innovation are needed to help organizations stay secure in an ever-evolving threat landscape.

Evaluating Network Security Effectiveness in Risk Management

A recurring theme in the literature is the importance of evaluating how effective network security measures truly are. Aksoy (2024) explored how organizational culture and leadership influence the success of network security efforts. Using the Technology-Organization-Environment framework, the study assessed how well an organization's security measures align with its broader goals and strategies. Similarly, Ahmadi (2024)

and Chen et al. (2023) emphasized the need to regularly evaluate proactive tools like Zero Trust Architecture and Role-Based Access Control to ensure they are still effective in blocking internal threats. These evaluations are vital for ensuring that security strategies remain aligned with an organization's risk management goals.

The key insight from Aksoy (2024) and Ahmadi (2024) is that IT managers must go beyond simply deploying security tools. They also need to continuously assess how well those tools are working, adapting them as needed to keep pace with evolving threats and compliance requirements. Regular evaluations are essential for maintaining resilience and effectiveness.

Adapting to Emerging Threats Through Risk Management

Another key theme is the need to adapt to emerging cyber threats. Otieno et al. (2023) emphasized the importance of constant monitoring and proactive risk identification in today's fast-changing technology landscape. Without ongoing updates and risk assessments, networks can quickly become vulnerable. Ahmadi (2024) and Chen et al. (2023) reinforced the value of proactive strategies, such as Zero Trust Architecture and Role-Based Access Control, which help limit damage from both internal and external attacks.

Integrated Cybersecurity Strategies: Technology, People, and Compliance

The literature also highlights the need for holistic cybersecurity strategies that combine advanced technology, human expertise, and regulatory compliance. Researchers recommend implementing tools like Zero Trust Architecture, deep packet inspection, and passwordless authentication to improve network security (Foreman et al., 2024; Oduguwa

& Arabo, 2024; Tomlinson et al., 2024). These tools not only address technical weaknesses but also improve early threat detection and enable proactive defenses.

Legal and ethical considerations are another key factor. Regulations like GDPR and HIPAA shape how data is managed and protected, especially in sectors such as healthcare and e-commerce (Morić et al., 2024; Pina, 2024). Studies also show that the psychological impact of data breaches, such as stress and anxiety, can affect employee decision-making during incidents (Sears & Cunningham, 2024), reinforcing the need for well-rounded planning that considers the human experience.

Barriers to Implementing Effective Network Security

Despite the need for better strategies, several barriers still limit the effectiveness of network security efforts. Cremer et al. (2024) and Khodadadyan et al. (2021) point to complex regulations as a major challenge, making it harder for IT managers to conduct thorough risk assessments or design effective security plans. Financial risks and regulatory pressure can also delay or prevent the implementation of necessary internal controls.

Otieno et al. (2023) noted that the pace of technological change itself is another challenge. As new threats emerge rapidly, IT managers must constantly update security protocols just to keep up. Khodadadyan et al. (2021), Cremer et al. (2024), and Otieno et al. (2023) collectively highlighted that, these barriers whether regulatory, external, or technological, require IT managers to adopt flexible and adaptive security strategies. Overcoming these barriers will require not only technological solutions but also regulatory compliance, external support, and continuous organizational adaptation.

Collaboration and Decision-Making in Network Security

According to Rikhardsson et al. (2021) and Aksoy (2024), effective collaboration and decision-making are crucial for implementing successful network security strategies. Rikhardsson et al. (2021) emphasized that, collaboration across departments is essential for adapting internal controls during crises. Aksoy, C. (2024). highlighted that, decision-making, supported by top management, is critical for the effective implementation of cybersecurity strategies. Khelil and Khlif (2022) also stressed that internal auditors play a key role in collaborative decision-making by providing insights into vulnerabilities and ensuring that controls are effective. The key findings of both researchers indicated that collaboration, both across departments and with top management is essential for creating a resilient network security strategy. Rikhardsson et al. (2021), Aksoy, C. (2024), and Khelil and Khlif (2022) suggested that IT managers must work closely with auditors, leadership, and other stakeholders to ensure that security controls are effectively implemented and maintained.

Improvements in Network Security

Several areas for improvement in network security emerge from the literature. Aksoy, C. (2024) emphasized the need for strong organizational support and culture to improve the effectiveness of cybersecurity measures. Ahmadi (2024) and Akhtar and Rawol (2024) highlighted the potential of AI and ML in enhancing network security, particularly in improving real-time threat detection. However, there is a gap in the literature in understanding how smaller organizations, with fewer resources, can adopt sophisticated internal control strategies like ZTA and RBAC. Additionally, more research

is needed to explore how AI and ML can be integrated into internal control frameworks to provide adaptive, dynamic security measures. By filling these gaps, future research can help IT managers create more robust security strategies that can respond to evolving threats in real-time.

Secure Networks From Cyberattacks

The selection of risk management and internal controls as central concepts in this study is justified by their direct relevance to the research question: how IT managers secure networks from cyberattacks. Risk management is essential for identifying and mitigating potential threats, while internal controls provide the necessary structure for enforcing security measures and reducing the risk of human error. Studies by Patterson et al. (2023) and Barraza de la Paz et al. (2023) emphasized that, without robust internal controls, even the most advanced technical defenses are vulnerable to failure due to human or procedural errors. In addition, the IST framework underscores the necessity of considering these concepts in a holistic manner, thereby emphasizing the value of a comprehensive approach to cybersecurity that incorporates both technological and organizational aspects. Addressing these two fundamental concepts, this paper fills a gap in the literature regarding holistic, systems-oriented approaches to cybersecurity.

From its literature, it is clear that network security strategies are complicated and keep changing since organizations are increasingly dependent on networked digital infrastructures. There has been an overall increase in the number of cybersecurity incidents worldwide, and cybercrime has become a major threat to the company's operation and data security (Barraza de la Paz et al., 2023). An important takeaway from

recent reports is that it is essential to include risk management and internal controls into holistic cyber-strategies (Liu et al., 2021). These approaches should not focus solely on technological defense mechanisms but also on the human factors, as user errors and disregard for security policies often act as the weakest links in the security chain (Kioskli et al., 2023).

Risk management is an important part of the network security process, including identifying, assessing, and treating risks. Research highlighted that risk management needs to be based on both technological and organizational controls, including but not limited to periodic audits, policy enforcement, and constant surveillance of network systems (Barraza de la Paz et al., 2023). Despite the attention that organizations have given to enhancing technical controls such as firewalls and encryption, shortfalls persist in confronting the human elements that compound security risks. For example, human mistakes are the common cause of more than 95 percent of security incidents, pointing to the requirement of effective training and awareness (Mishra et al., 2022).

The literature has also provided a critical assessment of internal controls, such as access control, auditing, and compliance, which serve to protect data integrity and system security. Yet internal control systems also have to accommodate the human dimension, in the sense that negligence or failure to follow policies creates gaps (Kioskli et al., 2023). Such controls, when adequately embedded with risk management practices, become part of an overall defense mechanism against emerging cybersecurity threats (Liu et al., 2021).

Recent surveys have also drawn attention to the impact of emerging technologies, including artificial intelligence-based cybersecurity tools, on improving threat detection and response times. Although Akhtar and Rawol (2024) encouraged the use of artificial intelligence in automating cybersecurity tasks, concerns remain about how to implement this technology within current infrastructures without increasing new vulnerabilities. This highlights the need for internal controls and risk management strategies that are adaptable and can integrate technological innovations while minimizing the potential risks these tools may introduce.

Risk management and internal controls have to be taken into account jointly in order to propose effective strategies to protect organizational networks from cyberattacks (Barraza de la Paz et al., 2023). The focus on IST in the literature highlights this interconnectivity, and that weaknesses in one area may impact the wider network of the organization (Liu et al., 2021).

Research With Similar and Differing Research Results

The studies ultimately suggest some degree of convergence in findings on the combination of risk management and internal control. A number of other works highlight the necessity of integrating these elements to successfully protect organizational networks. For instance, Khodadadyan et al. (2021) and Kioskli et al. (2023) present evidence that automated tools are not enough to handle risks, and that expert human judgment is required to deal with vulnerabilities. Similarly, Otieno et al. (2023) and Mishra et al. (2022) emphasize the important role of continuous monitoring and strong internal controls in preventing human error, which is often the primary cause of security

incidents. To sum up, these works support the idea that risk management and internal controls are related and should work together as an important part of a complete cybersecurity framework (Liu et al., 2021; Mishra et al., 2022).

On the other hand, divergent findings were revealed with respect to the efficacy of particular methods of risk management and internal control. For example, work like Ahmadi (2024) and Sarkar et al. (2022) suggests that technological solutions such as Zero Trust Architecture and Role-Based Access Control represent superior strategies for proactively preventing insider threats. This stands in contrast to findings that focus more on human knowledge. Otieno et al. (2023), for instance, emphasize the importance of continuous updates and monitoring in the dynamic software industry, where rapid technological changes make regular updates necessary to reflect new threats. In such fast-moving sectors, automated systems thrive and can adapt in near real time.

Transition and Summary

The literature review showed that, to confront cyber security issues, an integrated system is needed that combines risk management and internal controls. In this review, IST is positioned as a conceptual framework, underscoring the necessity for coherence between technical, organisational and human strategies. Research highlighted the significance of risk control in recognizing and eliminating vulnerability, and internal control with regard to access control, compliance audit, and staff training can effectively reduce the risks that emerge from human factor. Emerging technologies like AI-driven threat detection and Zero Trust Architecture (ZTA) offer promising advancements, yet they pose integration and scalability challenges for organizations, particularly in

resource-constrained environments. The synthesis of diverse sources identifies gaps in the literature, particularly regarding how IT managers operationalize these strategies where economic and organizational limitations present unique challenges. Addressing these gaps is essential to enhancing organizational resilience against evolving cyber threats. By focusing on integrating risk management and internal controls, this study contributes to a deeper understanding of practical strategies IT managers use to secure their organizations networks from cyberattacks.

Section 3 outlined the research methodology used to address the study's purpose. This includes the role of the researcher, ethical considerations in line with the Belmont Report, participant selection criteria, and data collection methods, such as semistructured interviews and document analysis. The section furthermore described the process of data analysis, the actions planned to validate and secure the reliability as well as the validity and confidentiality of the participant.

Section 4 summarized the findings of the study, and the data was analysed thematically. This chapter examined the means by which IT managers can merge risk management and internal controls to safeguard network security. The findings were aligned with the existing literature and conceptual framework, providing actionable recommendations for IT practitioners. Finally, Section 4 discussed the implications for positive social change, highlighting how improved cybersecurity practices can protect sensitive data, reduce the risks of cyberattacks, and foster trust in digital systems, contributing to a safer and more resilient digital environment.

Section 3: The Project

This section of the research project focused on the methodology that was employed in the research study; it also outlined the critical role of the project researcher in the data collection process. In this section, the researcher explored the various components of the selected research methodology, which included the population, sampling, participants, data collection activities, interview questions, data organizations, data analysis techniques, and lastly, the strategies that were used to ensure reliability and validity of this research study.

Project Ethics

As a researcher, my role is to ensure I manage the research process, which includes systemically gathering suitable data to help address my study's research question. The primary duty of the researcher is to help coordinate all the significant aspects of the research to help mitigate the risk of methodological failures occurring and have research quality; this includes recruiting participants, collection of data from the participants selected for the study lastly, analyzing the data collected to find answers to the study's research question (Busetto et al., 2020; Mwita, 2022). I selected and used the appropriate approach and techniques to help develop the necessary rapport and mutual orientation with the selected participants and collect data to help provide support for my study.

My relationship to this topic is deeply rooted in my professional experience as a Senior Security Consultant with over 20 years in IT and cybersecurity. I have spent a decade specializing in network security, vulnerability management, and compliance,

which has shaped my curiosity and commitment to understanding strategies for securing organizational networks from vulnerability attacks. My current role involves consulting for various organizations on IT governance, compliance, and risk mitigation strategies, allowing me to observe the challenges IT managers face in this domain. This research aligns with my career aspirations to enhance network security strategies and contribute to the field by bridging gaps in knowledge. Importantly, I do not hold any position of influence over potential participants, which minimizes concerns about positionality affecting the study (Yoon & Uliassi, 2022).

I adhered to the protocols established by the Institutional Review Board (IRB) to ensure that my research complies with ethical standards and follows the principles outlined in The Belmont Report (U.S. Department of Health & Human Services, 1979). These principles, respect for persons, beneficence, and justice guided my approach to participant selection, informed consent, and data protection. Before initiating the study, I secured IRB approval, providing evidence that my research plan safeguards participants' welfare, the approval number is 02-19-25-1194917.

Additionally, I communicated the study's purpose, procedures, and potential risks and benefits to participants, fostering transparency and respect. Measures to maintain confidentiality and protect participants' data were prioritized, including secure data storage and anonymization strategies.

Informed consent is a cornerstone of ethical research, and I obtained it from all participants before initiating any data collection activities. Participants received comprehensive information about the study, including its purpose, procedures, and their

rights, such as the voluntary nature of participation and the ability to withdraw at any time without penalty. The informed consent process involved reviewing the IRB-approved consent form with participants to ensure their understanding and address any questions. To protect confidentiality, pseudonyms replaced participants' names, and identifying details were removed from records. This process aligns with the principles of beneficence and respect for persons, ensuring ethical integrity throughout the study.

As the researcher, I ensured the ethical protection of all participants by implementing robust confidentiality and data security measures. Participants' identities were masked using codes such as P1, P2, etc., and raw data, including interview transcripts, were securely stored on encrypted drives for a minimum of five years, as required by Walden University's policies. At the end of this retention period, all data will be permanently deleted. These measures not only comply with ethical research guidelines but also reinforce participants' trust and confidence in the research process (Taquette & Borges da Matta Souza, 2022). Through careful adherence to ethical standards, I aim to produce findings that contribute meaningfully to the field of cybersecurity while upholding the rights and dignity of all participants (Miracle, 2016).

Nature of the Project

This research study employed a qualitative method because it aimed to explore strategies IT managers used to secure their organizations networks against cyberattacks. Qualitative research, focuses on exploring events, experiences, opinions, or concepts through non-numerical data such as text, audio, and video. The goal was to understand human behavior and context rather than to explain it statistically (M. Hennink & Kaiser,

2022). The qualitative method is suitable for this study as it focuses on understanding participants' experiences and contextual insights, aligning with the research objectives. I used a pragmatic inquiry design, which focuses on solving real-world problems and generating practical outcomes (Allemang et al., 2021). Pragmatic inquiry is particularly appropriate for addressing cybersecurity challenges, as it emphasizes actionable strategies and contextual understanding. Pragmatic inquiry was chosen because it aligns with the study's objectives, enabling an in-depth investigation of actionable strategies to network security challenges faced by IT managers.

Population, Sampling, and Participants

The population for this study included six to seven IT managers from enterprise organizations. The participants met the following eligibility criteria: (a) are IT Managers, (b) worked or working in the IT industry, and (c) have secured their organizations network from cyberattacks.

To achieve a meaningful selection of participants, I used purposive sampling to select at least six to seven participants. Purposeful sampling is an ideal method in qualitative research as it allows for the selection of individuals who can provide rich, relevant, and insightful data specific to the study's objectives (Bouncken et al., 2025; Hennink & Kaiser, 2021). Data saturation occurs when additional interviews no longer yield new themes or insights, ensuring the study's comprehensiveness and relevance (Hennink & Kaiser, 2021). The saturation point signified a satisfactory depth of data for analysis while maintaining flexibility throughout the research process. To achieve data saturation, I interviewed participants until no new information or themes emerge.

My strategy to gain access to participants included the use of the social media platform LinkedIn. LinkedIn provides access to a broad pool of IT professionals, ensuring that recruitment efforts target those who meet the eligibility criteria. Introductory messages outlined the purpose of the study, the ethical safeguards in place, and the participants' rights.

Data Collection Activities

Data collection is a critical component of qualitative research, as it ensures that information gathered is reliable, valid, and reflective of the participants' experiences. For this study, I acted as the primary data collection instrument, conducting semistructured interviews as the primary data collection method. Semistructured interviews are particularly suited for qualitative research because they balance structure with flexibility, allowing the researcher to explore in-depth insights while maintaining consistency across interviews (Belina, 2022). This method is ideal for exploring strategies employed by IT managers to secure their organizations' networks against cyberattacks.

To enhance the reliability of the data collection process, I followed an interview protocol (see Appendix C), which includes a set of open-ended questions designed to encourage detailed and thoughtful responses. Open-ended questions are beneficial because they allow participants to share their experiences and perspectives in their own words, leading to richer data and uncovering insights that closed-ended questions may overlook (Belina, 2022).

Interviews were conducted using secure video conferencing platforms such as Microsoft Teams or Zoom. These platforms provide convenience and accessibility while

maintaining the confidentiality of the participants. To ensure data security and minimize technical disruptions, all audio recordings were captured using two separate recording devices, which were tested prior to each session. This precaution helped mitigate the risk of data loss due to device malfunction. After recording the interviews, transcription software, such as Cockatoo, was used to convert the audio recordings into text. Transcriptions were then reviewed for accuracy, ensuring that the participants' responses are fully captured and correctly represented. NVivo Excel software was used to organize, code, and analyze the qualitative data, allowing for efficient identification of patterns and themes within the dataset (Allsop et al., 2022). To enhance the trustworthiness of the data, I employed member checking. This process involves sharing transcriptions and preliminary findings with participants to confirm their accuracy and ensure that their perspectives are represented correctly (Riazi et al., 2023).

The techniques used to collect data in qualitative research must align with the research objectives and design. For this study, the primary data collection techniques were semistructured interviews and document analysis. These techniques provided a robust framework for gathering in-depth insights into the strategies IT managers use to secure their organizations' networks.

Semistructured interviews were conducted via video conferencing platforms, which offered the flexibility of real-time interaction while minimizing logistical challenges (Palacios Martínez, 2020). Each interview lasted approximately 30–45 minutes, but I allocated 60 minutes to allow participants time to ask questions or provide additional insights. Open-ended questions guided the interviews, encouraging participants

to share detailed responses and enabling the exploration of unexpected themes or perspectives (Belina, 2022).

Document analysis supplemented the interview data, providing an additional layer of context and validation. In particular, three publicly available documents were reviewed to support and verify the findings and subthemes that emerged from the interviews:

Doc1 is *The NIST Special Publication 800-30: Guide for Conducting Risk Assessments* (Joint Task Force Transformation Initiative, 2012), which provides a comprehensive methodology for evaluating and mitigating cybersecurity risks. It directly supports subthemes such as automated risk assessments, vulnerability scanning, and post-attack analysis.

Doc2 is *The Cybersecurity Performance Goals* published by the Cybersecurity and Infrastructure Security Agency (CISA, 2023). This document outlines voluntary baseline practices for improving cyber resilience, including log monitoring, access control, and continuous vulnerability management, reinforcing subthemes like real-time threat detection and compliance-driven management.

Doc3 is the *MITRE ATT&CK Framework* (MITRE, 2023), which details adversarial tactics and mitigation strategies and is particularly relevant to subthemes such as predictive analytics, adaptive mitigations, and operational workarounds.

Additionally, publicly available documents, such as the *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1* by the National Institute of Standards and Technology (NIST), were reviewed to corroborate the strategies and practices discussed during the interviews. By combining interviews with publicly available

document analysis, I was able to cross-verify data from multiple sources, strengthening the study's overall reliability and comprehensiveness.

Before each interview, participants were reminded of their rights, including the ability to withdraw at any time without penalty. They were also informed about the use of audio recordings and asked for their consent to proceed. This process ensured transparency and fostered trust between the researcher and participants, leading to more candid and meaningful discussions (Hung et al., 2024).

Interview Questions

I used semistructured interviews to collect the data for my research. The interview questions included the following:

1. What strategies do you use to secure your organizations network(s) from cyberattacks?
2. How do you conduct risk assessments in your organization, and how do you decide which threats to address first?
3. What factors do you consider most critical when identifying cyberattack risks in your network security strategies?
4. How do you integrate external threat intelligence into your risk management practices to anticipate and prevent cyberattacks?
5. Can you describe a time when you had to adjust your risk management strategy in response to an evolving cyber threat?
6. How does your organization adapt to emerging threats?

7. What types of internal controls have you implemented to secure your organization's network, and how do you evaluate their effectiveness?
8. How do you ensure that internal controls such as access control, encryption, and multi-factor authentication are appropriately applied?
9. How do you address training staff to follow security protocols or prevent mistakes?
10. Can you share an example of a security incident where your internal controls helped secure your organization's network from a cyberattack?

These questions align with the research question by focusing on the strategies IT managers use to secure networks, integrate risk management measures, and implement effective internal controls. Additionally, they reflect the principles of the IST by examining systemic approaches to network security, emphasizing interconnected strategies, internal controls, and addressing the organizational dynamics that influence these approaches.

Data Organization and Analysis Technique

Proper data organization is essential for ensuring the integrity and accessibility of collected data throughout the research process. For this study, data were organized using Microsoft Excel, Onenote and OneDrive. OneNote served as a digital workspace for categorizing interview notes, transcriptions, and preliminary analyses. Its integration with other Microsoft Office applications makes it an ideal tool for managing research tasks and maintaining an organized workflow. Additionally, OneNote employs strong encryption protocols, such as 128-bit AES encryption, to secure sensitive data (Horsman,

2020). OneDrive provided secure, cloud-based storage for all digital data. This platform offers encryption for data at rest and in transit, ensuring the confidentiality and security of the collected information (Liu et al., 2021). Two-factor authentication further safeguard access to the data, reducing the risk of unauthorized breaches Chen et al. (2023). Physical documents, such as signed consent forms, were securely stored in a locked safe alongside an encrypted USB drive containing backup copies of the digital data. To maintain participant anonymity, each individual was assigned a unique identifier (e.g., P1 for Participant 1). Identifying information was stored separately from the data in an encrypted file. These measures ensures compliance with ethical guidelines and protect participants' privacy throughout the study. After five years, all data will be permanently deleted or destroyed in accordance with institutional policies.

Thematic analysis, supported by NVivo software, was the primary method for analyzing the qualitative data collected in this study. Thematic analysis is a systematic approach to identifying, analyzing, and interpreting patterns within qualitative data, making it particularly suitable for exploring the strategies employed by IT managers to secure their networks (Braun & Clarke, 2022). The analysis process began with familiarization, during which I reviewed interview transcripts to gain a comprehensive understanding of the data. This step allowed me to identify initial patterns and insights that informed subsequent stages of analysis (Braun & Clarke, 2023). Using NVivo, I coded the data into smaller units based on relevance to the research question. Coding involved categorizing data into meaningful groups, such as recurring themes, strategies, or challenges. These codes were then grouped into broader themes that reflect

participants' strategies and practices. NVivo's advanced tools streamlined this process, enabling efficient data organization and analysis (Paulus, 2023).

To validate findings, I employed methodological triangulation, comparing data from interviews to ensure consistency and reliability (Craig et al., 2021). Member checking further enhanced the credibility of the findings by allowing participants to review and confirm the accuracy of the interpretations. Data analysis continued until saturation was achieved, which occurred when no new themes or patterns emerged. This iterative process ensures a thorough and comprehensive understanding of the data, leading to robust and actionable findings (M. Hennink & Kaiser, 2022).

Reliability and Validity

Reliability is about consistency; it's about whether you're getting the same results each time, under similar conditions, thereby producing similar outcomes. In qualitative research, this concept is known as dependability, which is achieved by following a clear and transparent process for collecting and analyzing data (Storey et al., 2024). In this study, dependability was ensured through member checking. This involved asking participants to review their interview transcripts and the researcher's interpretations to make sure everything accurately reflected their views and experiences (Riazi et al., 2023).

Validity is about how accurate, believable, and trustworthy the findings are. In qualitative studies, validity is evaluated through several key elements: credibility, transferability, confirmability, and dependability (Zia Ul Haq et al., 2023). Credibility in this study was strengthened through methodological triangulation, this means that the

researcher compared data from different sources, such as interviews from different managers to see if they aligned. When different sources support the same conclusion, it increases the strength and trustworthiness of the results (Coleman, 2021). Member checking also played a role in boosting credibility, by giving participants the chance to confirm and clarify the findings, to ensure their experiences were correctly represented (Riazi et al., 2023).

Transferability

Transferability in research refers to the ability of findings from one study to be applied to other, similar contexts, situations, or populations and for this study, I described the context of the study in detail, including information about the participants and the research setting. These descriptions help readers decide whether the findings are relevant or applicable to their own environments (Braun & Clarke, 2023). Data saturation was reached when no new ideas or patterns emerged during interviews and document analysis. This ongoing, reflective process ensured that the main themes were thoroughly covered and that the data captured the full scope of the topic being studied (M. Hennink & Kaiser, 2022).

Credibility

Reflexive journaling was used to record personal biases and how they were mitigated, ensuring that the findings reflect the participants' experiences rather than the researcher's interpretations (Peddle, 2022). Methodological triangulation, using multiple data sources to validate findings, enhanced credibility by confirming results through different perspectives (Moon, 2019). Additionally, NVivo software supported the

organization, coding, and identification of themes, ensuring consistency and transparency in the analytic process (Allsop et al., 2022).

Confirmability

To establish confirmability and demonstrate that my research study's findings are grounded in the data and are not influenced by the researcher's bias, I used the following strategies during the interviews: I used the probing technique to help elicit detailed responses and clarify the participants' perspectives. Doing this helped ensure an accurate representation of their experiences. I conducted follow-up member-checking interviews; the data was triangulated from multiple sources, and I performed a reflexive commentary. Confirmability in qualitative research is defined as the degree to which the findings are shaped by data rather than the researcher's bias or preconceptions (Steltenpohl et al., 2022).

To ensure data saturation is established in this study, I collected data for the research participants iteratively using semistructured interviews. The iterative process involved reviewing the gathered data and using insights from the previous interviews to help inform subsequent data collection. I continued to collect data until no new themes or insights emerged and the collected information became redundant. Data saturation occurs when the issues and insights related to the phenomenon being studied start to repeat, making collecting more data redundant (M. Hennink & Kaiser, 2022). Reaching data saturation can help ensure credibility, transferability, and confirmability of my research's study findings.

Transition and Summary

In this study, I explored strategies IT managers use to secure their networks from cybersecurity attacks. I stated my IT problem and research purpose and described the qualitative pragmatic enquiry approach and the research-related ethics. I used IST as the conceptual framework for this doctoral study. I addressed the assumptions and limitations, explained the significance of this study, and reviewed professional and academic literature. In Section 4 of this study, I discussed the findings and the implications for business practices, social change, further research, and conclude with the study's overall contributions and insights.

Section 4: Application to Professional Practice and Implications for Change

Introduction

The purpose of this qualitative pragmatic inquiry was to explore strategies that IT managers use to secure their organizations' networks from cyberattacks. The overarching research question was: What strategies do IT managers use to secure organizational networks from cybersecurity attacks?

Overview of the Study

Data was collected through semistructured interviews consisting of ten open-ended questions outlined in the interview protocol (see Appendix), with seven IT managers who have successfully managed and secured enterprise networks from cybersecurity attacks. The seven IT Managers were recruited via LinkedIn invitation and my professional association and their responses provided rich qualitative data to address the overarching research question.

The interviews were audio recorded. Each study participant was provided with the participant consent form beforehand and had an opportunity to ask questions regarding the interview process before the interview sessions commenced. I informed each participant that participation in the research study interview was entirely voluntary, and they had a right to withdraw from the interview at any time. All interviews were conducted using Microsoft Teams and zoom; each session lasted between 20-35 minutes. I conducted member checking by sending a clean version by sending the transcribed clean version to participants via email to ensure participant information was accurately validated. participants made minor corrections and returned the updated version with

their consent to use as is. To provide anonymity, the seven participants were assigned a numeric code throughout the interview process: P1, P2, P3, P4, P5, P6, P7. Coding, thematic analysis and data organization storage were done using Microsoft Excel.

Presentation of the Findings

I commenced this study to understand the strategies IT Managers use to secure organizations' networks from cybersecurity attacks. To provide a structured view of the insights gathered, this section includes tables on Internal Control, Risk Management, and Thematic Analysis. These tables serve as critical analytical tools, illustrating how IT managers strategically implement security measures, assess risks, integrate intelligence, and mitigate cyber threats effectively. Grounded in the IST framework, these tables specifically support the two major pillars of the study: Internal Controls and Risk Management:

Internal Control Table

The internal control table provides a structured view of security controls, detailing how IT managers enforce access controls, encryption, compliance audits, and training to maintain organizational security. The table emphasize that effective cybersecurity requires a dynamic and interconnected control system, as emphasized in IST's principles.

Table 1*Internal Security Control Comparison*

Internal control factor	Prioritization criteria	Research results
Access control	Role-based access control (RBAC) enforces the least privilege and prevents unauthorized access.	Access to necessary resources
Multifactor authentication (MFA)	Required all employees to strengthen authentication security and reduce credential theft.	Mandatory MFA
Encryption policies	Encrypting sensitive company data to prevent data breaches and ensure confidentiality.	Sensitive data encrypted
Security audits	Continuous security assessments and external compliance audits to identify vulnerabilities.	Routine security audits
Regulatory compliance	Adherence to NIST, SOC, PCI DSS, and CIS standards to maintain security compliance.	Comply with security frameworks
Employee security awareness training	Phishing simulations and security training to reduce human-related risks.	Conduct phishing simulation

The order of implementation follows a layered security approach, prioritizing controls that provide immediate protection before enhancing long-term security governance:

1. Access Control is prioritized first because it establishes who has access to what in the system, ensuring unauthorized users are blocked from critical resources.
2. MFA is implemented immediately to secure authentication processes, reducing credential theft risks.
3. Encryption Policies come next to protect stored and transmitted data, ensuring confidentiality.
4. Security Audits follow, ensuring that all security measures are working effectively and identifying potential gaps.
5. Regulatory Compliance is addressed continuously but becomes a major focus after fundamental security controls are in place to meet industry standards.
6. Employee Security Awareness Training is ongoing but becomes more crucial once technical security controls are in place, ensuring that human risks (e.g., phishing) are minimized.

Risk Management and Thematic Analysis Tables

- The Risk Management Table categorizes and prioritizes risks based on financial, compliance, business continuity, user behavior, and third-party risks, showcasing how IT managers identify and mitigate vulnerabilities.

- The Thematic Analysis Table provides a deeper examination of the strategies used to secure their network from cyberattacks, aligning with IST’s emphasis on continuous risk assessment and proactive response mechanisms.
- These tables reinforce that risk management is not a static process but an adaptive approach that integrates threat intelligence, automated detection, and human factor considerations.

Table 2*Risk Management Strategy Comparison*

Risk factor	Prioritization criteria	Example quote
Financial risks	Prioritized to prevent fraudulent transactions and data theft.	Focus on biggest impact risks first
Compliance risks	Ensuring adherence to NIST R2, PCI DSS, and ISO 27001 frameworks.	Comply with industry standards
Business continuity risks	Mitigating ransomware and operational disruptions.	Focus on early detection
User behavior risks	Phishing awareness, credential security, and BYOD policy enforcement.	MFA and training
Third-party risks	External vendors, cloud security, and software supply chain vulnerabilities.	Assess external vendors

Thematic Summary

The qualitative analysis revealed eight core themes that collectively represent the multifaceted strategies IT managers use to secure organizational networks against cyber threats. These themes are grounded in participant responses and supported by observed codes and patterns across interviews and document analysis.

- Comprehensive Security Architecture focuses on building layered defenses through technologies like firewalls, intrusion detection systems (IDS), segmentation, and access controls to minimize the attack surface and enforce network integrity.
- Risk Assessment & Mitigation emphasizes proactive identification of vulnerabilities and risk prioritization using tools such as automated scans, log analysis, and temporary compensating controls to handle unpatched systems.
- User Security Training & Awareness underscores the human element in cybersecurity, highlighting the importance of phishing simulations, MFA enforcement, and scenario-based training to reduce user-driven threats.
- Threat Intelligence & Adaptive Defense captures the need for real-time visibility into threat patterns, leveraging government and commercial intelligence feeds, and adaptive controls to respond to evolving attack vectors.
- Security Governance & Compliance Enforcement reflects the operationalization of industry frameworks such as NIST, PCI DSS, and CIS through audits, access controls, and third-party security enforcement.

- Cyberattack Defense & Incident Management addresses the implementation of deception technologies like honeypots, automated rule enforcement, and structured response drills to contain and recover from breaches efficiently.
- Operational Technology (OT) & Industrial Security highlights the unique risks in industrial environments, advocating for IT/OT segmentation, specialized monitoring, and restricted vendor access in critical infrastructure contexts.
- Government Cybersecurity Standards & Zero Trust ties together the increasing influence of national frameworks (e.g., CISA, NIST, FISMA) and the adoption of Zero Trust principles that assume no implicit trust and enforce continuous verification.

Together, these themes demonstrate a holistic and adaptive approach to cybersecurity, rooted in best practices, regulatory alignment, and operational realities faced by modern IT leaders. See Table 3.

Table 3*Thematic Summary*

Themes	Description	Codes
1. Risk assessment & mitigation	Involves risk evaluations, vulnerability assessments, log analysis, and handling unpatched systems to prioritize risk-based decision-making.	Automated risk assessments, Log analysis, Prioritization of vulnerabilities, Temporary mitigations for unpatched systems, Compliance gap analysis
2. Security governance & compliance enforcement	Covers compliance frameworks (NIST, PCI DSS, CIS), security audits, and enforcing security standards across organizations.	Role-based access control (RBAC), Compliance audits, Vendor & client security policy enforcement, Removing insecure remote access methods
3. Comprehensive security architecture	Covers firewalls, IDS, segmentation, and geofencing, ensuring network defenses are layered and robust.	Firewall implementation, IDS/IPS, Network segmentation, Geofencing, Access Control Lists (ACLs), VPN & remote access analysis
4. User security training & awareness	Covers phishing training, MFA enforcement, and educating employees on security best practices to minimize human errors.	Phishing simulations, MFA enforcement, Credential security awareness, Security training with practical context, Incident escalation training
5. Threat intelligence & adaptive defense	Involves monitoring attack patterns, tracking zero-day threats, and leveraging government/private sector threat feeds.	Threat intelligence feeds, Monitoring attack vectors, Zero-day vulnerability tracking, Security vendor intelligence reports, MITRE ATT&CK framework

Themes	Description	Codes
6. Cyberattack defense & incident management	Focuses on deploying honeypots, automated firewall adjustments, geofencing for malicious traffic control, and structured incident response plans.	Honeypots for attacker deception, Automated firewall rule adjustments, Geofencing for real-time attack mitigation, Security incident response drills
7. Operational technology (OT) & industrial security	Addresses security risks in industrial environments (ICS & SCADA), requiring segmented access control and real-time monitoring.	ICS/SCADA security, IT/OT segmentation, Vendor access controls, Production network monitoring
8. Government cybersecurity standards & Zero Trust	Focuses on Zero Trust security, government compliance (FISMA, NIST, CISA), and national threat intelligence strategies.	Zero Trust architecture, Endpoint detection and response (EDR), CISA & DHS intelligence feeds, Government compliance enforcement.

By presenting internal controls and risk management strategies in a structured and comparative format, these tables provide empirical evidence of how IT managers balance compliance, security enforcement, and risk mitigation in cybersecurity decision-making. As the two pillars of this research, internal controls and risk management are central to understanding how organizations protect their systems and mitigate cyber threats, IST emphasizes that risk management, internal controls, technical infrastructure, internal policies, and security policies are all interdependent, meaning, a weakness in one area can compromise the entire organization. To maintain a robust cybersecurity posture, both

technological and human factors must function cohesively as part of an integrated defense system.

Findings and Thematic Focus

The analysis of interviews conducted with IT Managers with a minimum of five years' experience, revealed eight key themes related to strategies for securing organizational networks from cyberattacks. These themes emerged based on recurring patterns in participants' responses, reflecting critical areas of cybersecurity practices. The identified themes are as follows:

- risk assessment & mitigation
- security governance & compliance enforcement
- comprehensive security architecture
- user security training & awareness
- threat intelligence & adaptive defense
- cyberattack defense & incident management
- operational technology (OT) & industrial security
- government cybersecurity standards & Zero Trust

To validate and contextualize these themes, three publicly available documents were reviewed alongside the interview data: Doc1- *The NIST Special Publication 800-30: Guide for Conducting Risk Assessments (Joint Task Force Transformation Initiative, 2012)*. This document outlines comprehensive methodologies for evaluating and mitigating cybersecurity risks through structured risk assessment processes. Doc2: *The Cybersecurity Performance Goals (CISA, 2023)*- These goals offer voluntary, baseline

cybersecurity practices to enhance resilience, including log monitoring, access control, and vulnerability management. Doc3: The MITRE ATT&CK Framework (MITRE, 2023)- A globally recognized resource detailing adversarial tactics, techniques, and mitigation strategies based on real-world cyber threat intelligence. These documents were selected for their alignment with recognized government and industry standards and their direct relevance to the subthemes and practices described by participants. The triangulation of interview data with these authoritative sources strengthens the validity and credibility of the study's findings.

First Theme: Risk Assessment & Mitigation

A summary of the key subthemes, the frequency of mentions, participant involvement, and supporting documents related to risk assessment and mitigation is presented in Table 4.

Table 4*Subthemes in Risk Assessment & Mitigation Theme*

Subtheme	Participant count	Participant references	Document count	Document references
Automated risk assessment & vulnerability scanning	6	18	3	9
Real-time log monitoring & threat detection	5	14	2	6
Predictive analytics & AI-driven risk modeling	3	9	2	6
Compliance-driven risk management	5	12	2	6
Postattack analysis & adaptive mitigations	4	10	2	5
Temporary mitigations for unpatched systems	3	8	1	3
Balancing risk vs. operational constraints	2	5	1	2

Subtheme 1: Automated Risk Assessment & Vulnerability Scanning

Six participants (P1, P2, P3, P4, P5, and P6) emphasized that automated scanning tools were essential for identifying vulnerabilities quickly and prioritizing remediation before attackers could exploit them. They described automation as a foundational practice that improves visibility, reduces manual workload, and ensures potential risks are addressed before escalation. Barraza de la Paz et al. (2023) found that automation enhances detection speed and improves vulnerability prioritization in enterprise environments. This supports IST by showing how technology and processes work together to strengthen proactive defense.

Subtheme 2: Real-Time Log Monitoring & Threat Detection

Five participants (P1, P2, P3, P5, and P6) described real-time log monitoring as a crucial early warning mechanism that allowed them to detect suspicious activity and respond before incidents escalated. They shared that continuous visibility into network activity provided early alerts and actionable intelligence, significantly improving response times. Asasfeh et al. (2024) highlighted that continuous monitoring significantly improves early threat identification and response capability. Within IST, continuous monitoring acts as the connective layer that links human oversight, processes, and technology to enhance adaptive security.

Subtheme 3: Predictive Analytics & AI-Driven Risk Modeling

Three participants (P3, P5, and P6) shared that predictive analytics allowed their teams to anticipate emerging threats and take preventive action rather than reacting after an attack. They described AI-based modeling as an enabler of proactive defense, giving them the ability to respond before threats materialize. Asasfeh et al. (2024) demonstrated that AI-based analytics help detect abnormal behavior and reduce insider threat risks. This reflects IST's principle that interconnected systems must evolve proactively to stay ahead of dynamic threats.

Subtheme 4: Compliance-Driven Risk Management

Five participants (P2, P3, P4, P5, and P7) stressed that integrating compliance assessments and gap analyses into their risk management process ensured alignment with security standards and reduced audit risks. They reported that this approach not only improved regulatory readiness but also strengthened the overall security posture. Mayer

and Aubert (2021) reported that organizations linking compliance to risk management improve control effectiveness and overall resilience. This aligns with IST by demonstrating how organizational policy and technical safeguards must function as a unified system.

Subtheme 5: Postattack Analysis & Adaptive Mitigations

Four participants (P2, P4, P5, and P7) explained that analyzing incidents after they occurred helped refine their strategies and adapt future responses, making their defenses stronger over time. They emphasized that lessons learned from real-world incidents informed new policies, improved controls, and enhanced readiness for future threats. Mishra et al. (2022) found that organizations that integrate post-incident learning into their strategies experience fewer repeat breaches. This supports IST's emphasis on continuous feedback loops, where past experiences inform and strengthen future responses.

Subtheme 6: Temporary Mitigations for Unpatched Systems

Three participants (P1, P4, and P6) noted that when immediate patching wasn't possible, temporary solutions like network segmentation and access restrictions were vital to limit exposure. They explained that these stopgap measures allowed them to maintain operational security while awaiting permanent fixes. Barraza de la Paz et al. (2023) emphasized that dynamic mitigation strategies maintain security integrity when full remediation is delayed. This reflects IST's focus on flexibility and adaptation, ensuring system stability even when permanent solutions are not immediately available.

Subtheme 7: Balancing Risk Versus Operational Constraints

Two participants (P3 and P5) highlighted the need to balance strict security measures with operational realities, ensuring that protective actions did not disrupt essential business functions. They noted that effective risk strategies must align with business priorities to maintain both security and continuity. Mayer and Aubert (2021) observed that aligning risk management with business priorities leads to more sustainable security outcomes. This aligns with IST's emphasis on harmonizing technical measures with organizational goals to create a balanced and effective security posture.

The theme of Risk Assessment & Mitigation was foundational to an effective cybersecurity posture, especially in dynamic enterprise environments where threats evolved rapidly. Its importance lay in enabling organizations to proactively identify, evaluate, and respond to potential threats before they could be exploited. As highlighted by participants (P1–P7), a robust risk assessment process, coupled with mitigation strategies, empowered IT managers to move from reactive security to a proactive, resilient defense model. In particular, tools like automated vulnerability scanning, predictive AI modeling, and real-time log monitoring allowed for earlier detection and faster remediation. This approach reduced the attack surface and supported more informed security decision-making, ultimately enhancing organizational resilience. The theme also highlighted how integrating regulatory compliance, operational awareness, and technical insights provided a comprehensive risk management strategy. Furthermore, adaptive strategies such as temporary mitigations and post-incident learning ensured that organizations remained flexible and responsive in the face of constraints or novel attacks.

A structured risk assessment approach involved continuous log monitoring, vulnerability scanning, and prioritization of threats based on impact and exploitability. This aligned with Barraza de la Paz et al. (2023), who highlighted that an effective risk management strategy integrated both technical controls (e.g., automated log monitoring, IDS) and organizational policies (e.g., compliance audits and risk prioritization) to mitigate cyberattack risks before they escalated.

Security professionals utilized automated tools such as Qualys, Microsoft Defender, and threat intelligence feeds to detect anomalies in real time. P1 and P3 emphasized that real-time threat analysis enhanced cybersecurity resilience by allowing organizations to respond to threats before they became full-scale security incidents. P6 contributed to this discussion by emphasizing the role of predictive analytics in identifying emerging threats, stating that proactive AI-driven risk modeling was essential for modern cybersecurity strategies. This was supported by Asasfeh et al. (2024), who noted that AI-based behavioral analytics enabled real-time threat detection, significantly reducing the potential for insider attacks and improving cybersecurity resilience. P2, P5, and P7 reinforced the importance of compliance-driven risk management, emphasizing gap analysis, risk scoring methodologies, and regulatory compliance assessments to enhance security. This supported Mayer and Aubert (2021), who argued that organizations that integrated compliance frameworks into risk assessment improved security by enforcing standardized best practices.

Additionally, participants highlighted the role of post-attack analysis and continuous risk adaptation in strengthening security postures. P4 and P7 shared insights

on adapting risk strategies based on past incidents, stating that ransomware attacks often required adjustments in security response plans, particularly in how privileged access was managed. This aligned with Mishra et al. (2022), who found that organizations with dynamic risk management strategies experienced fewer security breaches due to their ability to quickly adapt to evolving cyber threats. The participant insights extended this knowledge by emphasizing temporary mitigations for unpatched systems, ensuring that known vulnerabilities were contained until permanent solutions were implemented.

To validate this theme and its subthemes, three public documents were reviewed and analyzed alongside participant responses to ensure alignment between real-world experiences and industry standards. This triangulation strengthened the study's credibility by demonstrating that participant insights were not isolated but reflected broader cybersecurity practices recognized by leading authorities. *The NIST Special Publication 800-30, Rev. 1 Guide for Conducting Risk Assessments (Joint Task Force Transformation Initiative, 2012)* provides a comprehensive methodology for evaluating and mitigating cybersecurity risks. It directly supported subthemes such as automated risk assessments, vulnerability scanning, and post-attack analysis, all of which were consistently emphasized by participants like P1, P3, and P7 who discussed using tools such as Qualys, Microsoft Defender, and post-breach learning processes. The *Cybersecurity Performance Goals (CISA, 2023)* outlined voluntary baseline practices for improving cyber resilience, including log monitoring, access control, and continuous vulnerability management. These elements directly reinforced participant responses (P2, P5, and P6) who highlighted the operational use of real-time log analytics, compliance

scoring models, and layered access policies to secure their network environments. The MITRE ATT&CK Framework (MITRE, 2023) detailed adversarial tactics, techniques, and mitigation strategies, and was particularly relevant to subthemes such as predictive analytics, adaptive mitigations, and operational workarounds. Participants P4 and P6 described the use of behavioral analytics, dynamic segmentation, and proactive containment mechanisms, which aligned directly with the adaptive defense concepts described in MITRE's framework.

The literature reviewed substantiated and expanded the significance of this theme, showing how a multi-layered and dynamic approach to risk assessment significantly reduced exposure to threats. Barraza de la Paz et al. (2023) emphasized the integration of log monitoring and compliance audits, Mayer and Aubert (2021) highlighted standardized best practices, Asasfeh et al. (2024) presented AI as a key enabler of real-time analysis, and Mishra et al. (2022) showed how post-breach adaptability strengthened the overall posture. These sources collectively validated participants' experiences, while also revealing a gap, namely, the operational challenges IT managers faced in applying these strategies in real-world environments.

The findings aligned with IST, which posited that risk management must be an interconnected and adaptive process rather than a standalone function. The integration of technical defenses, compliance policies, and real-time monitoring exemplified IST's principle that cybersecurity must function as a unified system, not as fragmented controls. By demonstrating how risk assessment tools, compliance audits, and response plans

worked cohesively, the findings supported IST's argument that security resilience required the seamless integration of risk management and technical safeguards.

The findings reinforced existing literature on proactive risk management and cybersecurity resilience. Organizations implementing real-time log monitoring, compliance-driven assessments, and continuous risk prioritization experienced fewer breaches and faster incident response times (Mayer & Aubert, 2021). The emphasis on temporary mitigations for unpatched vulnerabilities aligned with Barraza de la Paz et al. (2023), who argued that organizations must employ adaptive risk management strategies to handle unresolved security gaps dynamically.

However, a key insight from the findings was the practical challenge of balancing cybersecurity efforts with operational realities. P3 emphasized that real-time patching was not always feasible, necessitating temporary mitigations and strategic workarounds. This insight contrasted with traditional models of risk management that assumed full and immediate remediation was always possible. The findings suggested that flexible, operationally informed strategies were essential to maintain an effective security posture.

In conclusion, the theme of Risk Assessment & Mitigation remained a cornerstone of modern cybersecurity strategies. It was supported by both literature and public documentation, confirming that effective risk management must be dynamic, compliance-aware, and technologically integrated. The theme affirmed IST's central argument: effective cybersecurity emerged when all parts of the system, people, processes, and technology, worked in unison to anticipate, identify, and mitigate threats.

Second Theme: Security Governance & Compliance Enforcement

A summary of the key subthemes, participant involvement, and supporting documents related to Security Governance & Compliance Enforcement is presented in Table 5.

Table 5

Subthemes in Security Governance & Compliance Enforcement Theme

Subtheme	Participant count	Participant references	Document count	Document references
Role-based access control (RBAC)	4	10	2	5
Internal security policy enforcement	4	9	2	5
Third-party & vendor compliance management	4	11	2	6
Security governance integration into daily operations	3	7	3	8
Security audits & certification readiness	4	9	2	5
Adaptive/flexible compliance models	3	7	1	3
Cloud vendor & SaaS security compliance	2	5	2	4

Subtheme 1: Role-Based Access Control (RBAC)

Four participants (P2, P3, P4, and P6) emphasized that implementing role-based access control was essential to reducing unauthorized access and enforcing the principle of least privilege. They described RBAC as a foundational governance control that ensures users only have access to the resources required for their roles, significantly reducing potential attack surfaces. CISA (2023) underscored the importance of access control as a baseline performance goal for strengthening organizational security. This

aligns with IST, as RBAC demonstrates how governance policies and technical controls must work together to prevent vulnerabilities within a connected security system.

Subtheme 2: Internal Security Policy Enforcement

Four participants (P2, P3, P5, and P7) discussed how actively enforcing internal security policies was crucial for maintaining compliance and preventing policy drift. They explained that policies must not remain static documents but instead guide day-to-day decisions and shape employee behavior across the organization. Cheong et al. (2021) highlighted that compliance should be embedded in everyday operations rather than treated as a one-time exercise. Within IST, policy enforcement reflects the integration of people, process, and technology into a unified governance system, ensuring continuous alignment with organizational security objectives.

Subtheme 3: Third-Party & Vendor Compliance Management

Four participants (P2, P4, P6, and P7) emphasized the critical importance of holding vendors and third parties to the same compliance standards as internal operations. They noted that weak vendor security controls often introduce risks beyond an organization's direct control, making consistent oversight essential. Mayer and Aubert (2021) reinforced the necessity of enforcing vendor compliance, while Chang et al. (2021) warned of vulnerabilities arising from insufficient oversight. This supports IST's view that organizational security extends beyond internal boundaries, requiring external partners to integrate into the same interconnected compliance ecosystem.

Subtheme 4: Security Governance Integration into Daily Operations

Three participants (P3, P4, and P6) stated that security governance is most effective when integrated into daily workflows instead of existing as a separate or periodic process. They described embedding compliance checks into operational tasks, change-management processes, and system updates to ensure continuous alignment with standards. Barraza de la Paz et al. (2023) argued that governance must align with business operations to remain effective without hindering agility. This aligns with IST's principle that governance must function as a continuous, adaptive layer within the broader operational ecosystem.

Subtheme 5: Security Audits & Certification Readiness

Four participants (P2, P3, P5, and P7) highlighted regular security audits and certification readiness assessments as vital to maintaining compliance and demonstrating trust to clients and regulators. They explained that proactive audit preparation helps uncover gaps before formal reviews and ensures that compliance processes evolve alongside changing requirements. Mayer and Aubert (2021) emphasized the value of continuous audit readiness as part of a mature compliance program. From an IST perspective, regular audits act as a feedback loop that connects policy, control implementation, and real-world validation, strengthening the overall security system.

Subtheme 6: Adaptive/Flexible Compliance Models

Three participants (P2, P5, and P6) emphasized the need for compliance frameworks that can adapt to evolving threats and changing business environments. They described rigid, checklist-based approaches as insufficient and highlighted the importance

of tailoring controls to real-world risk conditions. Barraza de la Paz et al. (2023) supported the importance of operational flexibility, while Ambreen et al. (2024) argued for adaptive, risk-based compliance strategies. This reflects IST's emphasis on dynamic systems that evolve in response to environmental changes, ensuring continuous alignment between compliance requirements and organizational needs.

Subtheme 7: Cloud Vendor & SaaS Security Compliance

Two participants (P5 and P6) explained that ensuring cloud vendors and SaaS providers meet compliance requirements was essential as organizations increasingly rely on third-party infrastructure. They noted that shared responsibility models require careful monitoring and contractual enforcement to maintain compliance across distributed environments. Chang et al. (2021) highlighted the risks of inadequate vendor oversight, particularly in cloud environments. This aligns with IST by extending governance beyond internal systems, integrating external providers into the same continuous compliance network.

The theme of Security Governance & Compliance Enforcement highlighted the essential role that cybersecurity governance frameworks and compliance mandates played in strengthening organizational resilience. In cybersecurity management, governance established the policies, controls, and processes that protected critical assets, while compliance enforcement ensured these frameworks aligned with external standards such as NIST, PCI DSS, SOC 2, and CIS benchmarks. Participants (P2, P7) consistently emphasized that compliance must not be treated as a passive exercise but as an active, enforced component of daily operations. P3, P4, and P6 highlighted that role-based

access control (RBAC), security audits, and third-party compliance mandates were necessary to prevent gaps and vulnerabilities. P6 particularly stressed the operational tension that arose when compliance rigidity conflicted with business agility, underscoring the need for a flexible approach. This aligned with Barraza de la Paz et al. (2023), who noted that effective security governance must integrate into operational workflows without impeding business functionality. By enforcing compliance dynamically and extending its reach to vendors and third parties, participants demonstrated a commitment to comprehensive security governance beyond internal boundaries.

To validate this theme and its subthemes, three public documents were reviewed and analyzed alongside participant responses to ensure alignment between real-world experiences and industry standards. This triangulation strengthened the study's credibility by demonstrating that participant insights were not isolated but reflected broader cybersecurity practices recognized by leading authorities.

The NIST Special Publication 800-30 , Rev. 1 Guide for Conducting Risk Assessments (Joint Task Force Transformation Initiative, 2012) provided a structured methodology for integrating risk management with governance, emphasizing the need for ongoing compliance assessments that mirrored participants' focus on daily, operationalized security practices. This directly supported participant insights from P3, P4, and P6, who discussed the critical importance of embedding compliance enforcement into day-to-day operations rather than treating it as a periodic audit exercise. The *Cybersecurity Performance Goals (CISA, 2023)* outlined baseline cybersecurity performance goals, such as continuous log monitoring, access control, and vendor risk

management. These elements directly reinforced participant responses from P2, P5, and P7, who highlighted the necessity of implementing RBAC, real-time log monitoring, and third-party compliance oversight to strengthen organizational security postures. The MITRE ATT&CK Framework (MITRE, 2023) mapped adversarial tactics against defensive controls, supporting participant emphasis on embedding compliance and governance practices into operational monitoring, threat detection, and incident response strategies. Participants P5 and P6 described implementing continuous threat detection, adaptive policy enforcement, and integrating security monitoring directly into compliance frameworks, aligning closely with the defensive strategies outlined in the MITRE ATT&CK framework.

The literature reviewed substantiated and expanded the importance of security governance and compliance enforcement. Cheong et al. (2021) advocated that compliance must be integrated into everyday security operations, a point echoed by P3 and P4. Mayer and Aubert (2021) reinforced the necessity of enforcing third-party compliance, aligning with P2 and P7's concerns about vendor-induced vulnerabilities. Barraza de la Paz et al. (2023) emphasized operational flexibility in compliance, directly supporting P6's view that rigid compliance structures could disrupt business. Ambreen et al. (2024) argued for adaptive, risk-based compliance models, addressing the emerging need for dynamic compliance enforcement strategies. Chang et al. (2021) highlighted the risks of insufficient vendor compliance, which participants cited as a critical gap. Collectively, these sources not only validated participant experiences but also revealed critical gaps in traditional compliance models, namely, the failure to evolve compliance

from a certification-centric model to a proactive governance practice integrated into real-time operations.

The findings aligned with IST, which advocated for security management as a unified, interconnected system rather than a collection of independent controls.

Participants emphasized that compliance enforcement must be integrated into access control, monitoring, risk assessment, and vendor management practices, not treated as a separate or isolated activity. This supported IST's principle that security governance, compliance frameworks, and technical defenses must function cohesively to achieve true resilience. By embedding compliance into the broader cybersecurity ecosystem and treating it as a dynamic, continuously adaptive process, participants demonstrated the systemic thinking that IST promoted.

In conclusion, the theme of Security Governance & Compliance Enforcement remained a cornerstone of resilient cybersecurity strategies. Supported by both participant insights and existing literature, it confirmed that security governance must be dynamic, integrated into daily operations, and extended across organizational boundaries. Adaptive compliance strategies that balanced business needs with risk management emerged as critical for modern cybersecurity programs. This theme reinforced IST's principle that cybersecurity is not a collection of independent activities, but a dynamic, interconnected system where governance, monitoring, compliance, and response processes continuously evolved to meet emerging threats.

Third Theme: Comprehensive Security Architecture

A summary of the key subthemes, participant involvement, and document alignment is presented in Table 6.

Table 6

Subthemes in Comprehensive Security Architecture Theme

Subtheme	Participant count	Participant references	Document count	Document references
Centralized security architecture design	5	12	3	7
Segmentation and control zones	4	10	2	5
Automation and policy consistency	4	9	2	5
Unified monitoring and threat detection layers	3	8	2	6
Architectural support for incident response	3	7	1	4

Subtheme 1: Centralized Security Architecture Design

Five participants (P1, P2, P3, P5, and P6) emphasized that a centralized architectural design is the backbone of a strong cybersecurity program. They explained that building a cohesive architecture before deploying tools provides visibility, simplifies control management, and ensures the environment can adapt to evolving threats. Barraza de la Paz et al. (2023) highlighted that centralized security architectures reduce exposure and streamline response workflows.

This reflects IST by showing how a unified design connects people, processes, and technology into a cohesive, resilient defense structure.

Subtheme 2: Segmentation and Control Zones

Four participants (P1, P3, P5, and P6) described network segmentation and control zoning as critical to limiting lateral movement and containing potential breaches. They explained that dividing the network into isolated segments with tailored access controls significantly reduces the blast radius of an attack and improves monitoring accuracy. CISA (2023) reinforced the importance of segmentation as a best practice for containing threats and enforcing layered defenses. Within IST, segmentation illustrates how dividing complex systems into smaller, manageable units enhances systemic resilience and strengthens coordinated security responses.

Subtheme 3: Automation and Policy Consistency

Four participants (P2, P3, P4, and P5) highlighted automation and consistent policy enforcement as essential components of effective architectural design. They noted that automated policy application reduces configuration drift, minimizes human error, and ensures that security controls remain aligned across the enterprise environment. Ambreen et al. (2024) argued that automated processes strengthen adaptability and allow organizations to respond proactively to evolving threats. This aligns with IST's principle that integrated technological processes should function dynamically and consistently to maintain system reliability and effectiveness.

Subtheme 4: Unified Monitoring and Threat Detection Layers

Three participants (P1, P3, and P6) emphasized the value of unified monitoring and multi-layered detection as part of a comprehensive architecture. They explained that integrating visibility across network, endpoint, and application layers reduces blind spots

and speeds up incident detection. Barraza de la Paz et al. (2023) supported this by showing that layered monitoring improves detection accuracy and reduces vulnerabilities. From an IST perspective, unified monitoring illustrates the interconnected nature of modern defense, where multiple layers work together to detect, correlate, and respond to threats as a single system.

Subtheme 5: Architectural Support for Incident Response

Three participants (P2, P3, and P5) described how well-designed architecture provides critical support for incident response by streamlining communication paths, improving data correlation, and enabling rapid containment actions. They emphasized that proactive architectural planning allows incident response teams to act more quickly and effectively during crises. Ambreen et al. (2024) emphasized that architecture anticipating evolving threats enables faster, more efficient responses to incidents. This aligns with IST's concept of systemic integration, where architecture acts as the foundation that ties together detection, containment, and response capabilities into a unified whole.

The theme of Comprehensive Security Architecture highlighted the necessity of a layered, organization-wide security framework that integrated network, endpoint, application, and data-level defenses into a cohesive structure. Participants described how a well-defined architecture established zones of control, enforced segmentation, and integrated monitoring and access controls across the IT ecosystem. P1 and P5 emphasized that architectural planning was foundational to security and must precede any security tool deployment, ensuring long-term adaptability and resilience. This

observation supported Ambreen et al. (2024), who argued that resilient architectures enabled organizations to anticipate and respond to cyber threats proactively rather than reactively. P3 and P6 reinforced that without a comprehensive architectural foundation, organizations often experienced visibility gaps and delays in threat detection due to siloed and fragmented security deployments.

The findings confirmed and extended prior research advocating for defense-in-depth and systemic integration in cybersecurity design. Literature supported that centralized, unified security architectures reduced vulnerability exposure and simplified response workflows (Barraza de la Paz et al., 2023). Participants' emphasis on automation, segmentation, and centralized monitoring extended this knowledge by identifying specific architectural mechanisms that improved not only security detection but also operational efficiency across the enterprise.

To validate this theme and its subthemes, three public documents were reviewed and triangulated with participant responses. The NIST Special Publication 800-30, Rev. 1 Guide for Conducting Risk Assessments (Joint Task Force Transformation Initiative, 2012) supported the structured risk-based architectural planning emphasized by P1 and P5, who stressed that security must be incorporated into infrastructure design before deployment began. The Cybersecurity Performance Goals (CISA, 2023) reinforced the operational goals mentioned by P3 and P6, such as segmentation, real-time monitoring, and continuous control enforcement across IT systems. Participants' focus on continuous monitoring, centralized policy management, and layered control zones directly aligned with CISA's recommended cybersecurity practices. The MITRE ATT&CK Framework

(MITRE, 2023) validated the importance of creating integrated monitoring and adaptive defense structures, reflecting P3's and P6's emphasis on visibility layers and rapid response enablement. These documents collectively confirmed that the participant strategies aligned with best-practice architectural frameworks recognized in industry standards.

The literature reviewed substantiated the need for comprehensive security architecture. Barraza de la Paz et al. (2023) promoted centralized monitoring and the integration of security layers to reduce organizational vulnerability, supporting the participants' experiences. Ambreen et al. (2024) argued that architectures that anticipated evolving threats enabled faster and more efficient responses, mirroring participant insights regarding proactive adaptability. Frameworks such as Zero Trust Architecture also validated the need for dynamic, integrated design, emphasizing that compartmentalization and consistent monitoring enhanced incident response and reduced security risks.

The findings aligned closely with IST, which posited that resilience arose from the interconnected operation of multiple subsystems rather than isolated security controls. Participants' descriptions of architecture as the "spine" of cybersecurity directly mirrored IST's emphasis on the systemic integration of people, technology, and processes. Security architecture, as detailed by participants, tied together detection, access control, incident response, and governance into a seamless ecosystem, confirming IST's model of cohesive, adaptive system resilience.

In conclusion, Comprehensive Security Architecture was a foundational element of modern cybersecurity resilience. Validated through participant experiences, public documentation, and academic literature, this theme confirmed that integrated architectural designs were critical for reducing vulnerabilities, enhancing incident response, and ensuring long-term security adaptability.

Fourth Theme: User Security Training & Awareness

A summary of the key subthemes, participant involvement, and document alignment is presented in Table 7.

Table 7

Subthemes in User Security Training & Awareness Theme

Subtheme	Participant count	Participant references	Document count	Document references
Phishing simulation and attack response	4	10	2	6
Continuous cybersecurity training programs	5	13	2	7
Behavior retention and scenario-based learning	4	11	2	6
Security-conscious organizational culture	3	9	1	5
Integration of training into daily workflows	3	8	1	4

Subtheme 1: Phishing Simulation and Attack Response

Four participants (P2, P3, P4, and P6) emphasized the importance of regular phishing simulations as a frontline defense against social engineering. They explained that repeated simulations significantly reduced users' likelihood of clicking malicious links and improved response times during real incidents. Melaku (2023) reported that human error accounts for the majority of cybersecurity incidents, while Mishra et al. (2022) found that targeted awareness efforts reduce insider threats and social engineering risks. This aligns with IST, demonstrating that proactive training interventions strengthen the human layer of security, which is critical to the overall resilience of the system.

Subtheme 2: Continuous Cybersecurity Training Programs

Five participants (P1, P2, P3, P4, and P6) stressed the need for ongoing, continuous security training rather than one-time awareness sessions. They explained that continuous learning helps employees stay ahead of emerging threats, retain critical knowledge, and apply security best practices consistently. Mishra et al. (2022) supported this approach by showing that sustained awareness programs build long-term resilience against internal and external threats. Within IST, continuous training reinforces the principle that people must evolve alongside technological and procedural defenses to maintain a balanced and adaptive security posture.

Subtheme 3: Behavior Retention and Scenario-Based Learning

Four participants (P2, P3, P5, and P6) highlighted that scenario-based exercises significantly improved retention and real-world application of cybersecurity principles. They explained that realistic simulations and contextual training enabled users to better

recognize threats, make faster decisions, and apply policies effectively under pressure. Melaku (2023) emphasized that human behavior is a major factor in breaches, while Mishra et al. (2022) demonstrated that hands-on learning reinforces long-term security habits. This reflects IST's emphasis on integrating the human component into the broader security system, ensuring that individual behavior complements and strengthens technical controls.

Subtheme 4: Security-Conscious Organizational Culture

Three participants (P2, P4, and P6) explained that building a security-aware culture was just as important as technical defenses. They described how leadership messaging, communication, and visible executive support created an environment where employees felt responsible for safeguarding data and systems. Melaku (2023) supported this finding by highlighting that cultivating a security-focused culture reduces the likelihood of human errors leading to breaches. From an IST perspective, a culture of security awareness demonstrates how human behavior, organizational processes, and technology must work together as interdependent subsystems to achieve resilience.

Subtheme 5: Integration of Training Into Daily Workflows

Three participants (P2, P3, and P6) emphasized that integrating training into daily operations, such as onboarding, routine updates, and collaborative platforms, makes cybersecurity awareness part of normal work behavior rather than a separate, occasional activity. They explained that embedding reminders and micro-training into existing workflows improved engagement and reinforced security habits over time. Mishra et al. (2022) supported the importance of embedding training within regular business processes

to ensure that awareness becomes a continuous part of organizational operations. This supports IST's view that human, procedural, and technical elements must operate as one unified system to create sustainable security practices.

The theme of User Security Training & Awareness emphasized the crucial role of human behavior in securing organizational assets. Participants highlighted that without informed and security-conscious employees, technical controls were insufficient. This theme spanned regular security training, phishing simulations, and cultivated an organizational culture centered around cybersecurity awareness. P2 and P4 emphasized that recurring phishing simulations dramatically reduced user susceptibility to social engineering attacks, while P3 and P6 emphasized the need for ongoing, scenario-based training tailored to evolving threats. These observations aligned with Melaku (2023), who reported that over 90% of security incidents stemmed from human error, and Mishra et al. (2022), who argued that sustained awareness programs dramatically reduced insider threat risks. The findings confirmed existing literature that posited cybersecurity awareness as one of the most cost-effective strategies to reduce organizational risk. However, participant insights extended this understanding by highlighting the importance of retention, contextual learning, and integrating training into daily workflows and onboarding processes, moving beyond traditional compliance models toward continuous behavior reinforcement.

To validate this theme and its subthemes, three public documents were reviewed in conjunction with participant experiences. *The NIST Special Publication 800-30: Guide for Conducting Risk Assessments (Joint Task Force Transformation Initiative, 2012)*

reinforced the risk management approach supported by P2 and P4, who emphasized the importance of security awareness training to mitigate insider threats and phishing risks. The *Cybersecurity Performance Goals* (CISA, 2023) aligned with the practices described by P3 and P6, particularly the integration of workforce training, phishing defense, and continuous engagement strategies. These documents validated the participants' focus on incorporating security awareness into organizational culture and daily activities. The MITRE ATT&CK Framework (MITRE, 2023) highlighted user behavior as a key attack vector, supporting P2's and P3's emphasis on contextual, adaptive training methods designed to combat real-world attack techniques.

The literature supported these findings strongly. Melaku (2023) highlighted the outsized role human error played in breaches, while Mishra et al. (2022) advocated for sustained awareness initiatives to build long-term resilience. Participants' emphasis on practical, scenario-based training extended these scholarly insights by illustrating how learning retention and continuous application improved real-world defensive behaviors. The findings contributed by suggesting that organizations must move beyond static training models and adopt flexible, evolving programs that addressed emerging cyber risks dynamically.

The findings aligned perfectly with IST, which asserted that the failure of any subsystem, including human users, could compromise the overall system. Participants' emphasis on fostering a security-conscious workforce mirrored IST's notion that

sustainable cybersecurity resilience was only achievable when technical, procedural, and human components were fully integrated and aligned.

In conclusion, User Security Training & Awareness was fundamental to achieving holistic cybersecurity resilience. The findings, validated by participant experiences, public cybersecurity standards, and scholarly literature, confirmed that dynamic, engaging, and behaviorally focused training programs must be integrated into organizational practices to effectively manage cyber risks.

Fifth Theme: Threat Intelligence & Adaptive Defense

A summary of the key subthemes, participant involvement, and document alignment is presented in Table 8.

Table 8

Subthemes in Threat Intelligence & Adaptive Defense Theme

Subtheme	Participant count	Participant references	Document count	Document references
Integration of external threat intelligence	4	10	3	8
Adaptive security configuration based on threats	4	9	2	6
Automated threat detection and response systems	3	8	2	5
Intelligence-driven risk scoring and prioritization	3	7	1	4
Behavioral analytics and predictive defense	2	5	1	4

Subtheme 1: Integration of External Threat Intelligence

Four participants (P1, P3, P4, and P7) emphasized that integrating external threat intelligence was essential to understanding adversary behavior and anticipating emerging

risks. They described how consuming threat feeds from sources such as the MITRE ATT&CK framework and national cybersecurity centers allowed them to adapt defenses before threats materialized. P4 noted that intelligence sharing gave their team “early visibility into tactics,” while P1 highlighted that mapping these insights to their controls reduced blind spots across the network. Y. Zhang (2023) supported this approach, arguing that modern defense strategies must leverage external intelligence to stay ahead of sophisticated attackers. This aligns with IST, demonstrating how incorporating external intelligence strengthens the interconnected operation of detection, prevention, and response systems.

Subtheme 2: Adaptive Security Configuration Based on Threats

Four participants (P1, P3, P4, and P7) explained that their security controls were not static but continuously adjusted based on current threat intelligence. They described scenarios where firewalls, access policies, and segmentation rules were automatically updated in response to new attack campaigns. P3 noted that these adjustments “shut down attack paths before they were exploited,” and P7 emphasized that adaptive defenses “significantly reduced dwell time” during incidents. Mishra et al. (2022) found that integrating intelligence into defense strategies accelerates both detection and containment, improving the speed and effectiveness of response. Within IST, adaptive configurations illustrate the principle that security systems must evolve dynamically in response to environmental changes to maintain resilience.

Subtheme 3: Automated Threat Detection and Response Systems

Three participants (P2, P4, and P7) highlighted the value of automation in rapidly detecting and neutralizing threats. They described how automated systems adjusted firewall policies, isolated endpoints, and launched containment actions without requiring manual intervention. P4 explained that automation “buys critical time” for analysts, while P2 noted that it “reduces human error during high-pressure incidents.” Mishra et al. (2022) reinforced that automation significantly enhances the speed and accuracy of threat containment, turning intelligence into immediate action. This reflects IST’s emphasis on tightly integrated subsystems, where automated detection, analytics, and response mechanisms work in unison to form a self-adapting defense layer.

Subtheme 4: Intelligence-Driven Risk Scoring and Prioritization

Three participants (P1, P3, and P6) explained that they used threat intelligence to prioritize vulnerabilities and allocate resources effectively. By scoring risks based on real-world threat activity and potential impact, they focused mitigation efforts where they mattered most. P3 emphasized that this “moved the team from reactive patching to proactive defense,” and P6 highlighted that prioritization “aligned security investments with actual risk.” Y. Zhang (2023) supported intelligence-based prioritization, noting that it transforms traditional defense into a predictive model tailored to evolving adversarial tactics. This approach illustrates IST’s concept of coordinated decision-making across subsystems, where intelligence informs risk assessment, mitigation, and governance activities.

Subtheme 5: Behavioral Analytics and Predictive Defense

Two participants (P4 and P7) described how behavioral analytics enhanced their ability to detect subtle anomalies that might indicate insider threats or advanced persistent attacks. They explained that predictive defense models, built from historical behavior patterns, allowed them to spot and contain suspicious activities earlier in the attack chain. P7 remarked that predictive analytics “often reveal threats traditional signatures miss,” while P4 noted that it “turns raw data into actionable foresight.” Y. Zhang (2023) emphasized that predictive, intelligence-led defense is critical for countering sophisticated adversaries before they execute their attacks. This aligns with IST’s principle of continuous adaptation, showing how proactive data-driven insights integrate with broader security functions to enhance systemic resilience.

The theme of Threat Intelligence & Adaptive Defense highlighted the necessity for cybersecurity strategies that were predictive, intelligence-driven, and dynamic. Participants emphasized that traditional static defenses were no longer sufficient. Instead, organizations must have incorporated real-time threat intelligence, behavioral analytics, and automated adaptation of defenses to counter evolving threats. P1 and P4 discussed leveraging external threat feeds like MITRE ATT&CK and national cybersecurity centers to understand attacker behavior and adjust defense strategies accordingly. P3 and P7 reinforced the operational importance of adaptive defense, emphasizing the use of automated systems that revised firewall rules or isolated endpoints in real time based on the latest threat insights. These findings aligned with Y. Zhang (2023), who argued that

modern cybersecurity must move toward predictive, intelligence-led models to effectively combat sophisticated threat actors.

The findings confirmed and extended prior research advocating for intelligence-led, adaptive cybersecurity frameworks. Literature supported integrating real-time threat feeds with automated systems to accelerate detection and containment (Mishra et al., 2022). Participants' insights extended this understanding by illustrating how threat intelligence was operationalized daily through dynamic reconfiguration of security controls, resulting in more responsive and resilient defense postures.

To validate this theme and its subthemes, three public documents were reviewed alongside participant responses. *The NIST Special Publication 800-30: Guide for Conducting Risk Assessments (Joint Task Force Transformation Initiative, 2012)* supported the risk-based integration of threat intelligence into cybersecurity planning, as described by P1 and P4, who emphasized strategic architectural adjustments based on threat insights. The *Cybersecurity Performance Goals (CISA, 2023)* aligned with P3 and P7's focus on automated responses, adaptive firewall configurations, and intelligence-led defense strategies, emphasizing continuous threat monitoring and real-time system adjustments. The MITRE ATT&CK Framework (MITRE, 2023) reinforced the participants' operationalization of threat intelligence for detection and mitigation, confirming how participants like P4 and P7 mapped real-world attacker behaviors to defensive tactics and automated playbooks. These documents collectively validated that participants' approaches reflected recognized best practices in cybersecurity resilience.

The literature reviewed substantiated the theme's importance. Y. Zhang (2023) emphasized that static, perimeter-based security models were insufficient against modern threat actors, advocating for adaptive, intelligence-led models. Mishra et al. (2022) similarly emphasized that predictive threat intelligence integration led to faster detection and more effective responses. Participants' insights advanced this discourse by providing real-world examples of how threat intelligence was dynamically infused into security operations daily, leading to real-time adjustments and improved threat containment.

The findings aligned tightly with IST, which posited that cybersecurity resilience arose from the coordinated operation of interconnected subsystems. Participants demonstrated that integrating threat intelligence across detection, response, and mitigation workflows enabled systems to adapt and respond dynamically to evolving threats, confirming IST's model of cybersecurity as a living, adaptive ecosystem.

In conclusion, Threat Intelligence & Adaptive Defense was an essential component of modern cybersecurity resilience. The findings, validated through public documentation and academic literature, confirmed that predictive, intelligence-driven security strategies were critical to combating sophisticated cyber threats.

Sixth Theme: Cyberattack Defense & Incident Management

A summary of the key subthemes, participant involvement, and document alignment is presented in Table 9.

Table 9*Subthemes in Cyberattack Defense & Incident Management Theme*

Subtheme	Participant count	Participant references	Document count	Document references
Structured incident response planning	4	10	3	7
Cyberattack simulation and tabletop exercises	3	9	2	6
Deception and honeypot technologies	3	8	2	5
Automated containment and recovery systems	3	7	2	5
Integration of response and detection systems	2	5	1	4

Subtheme 1: Structured Incident Response Planning

Four participants (P2, P3, P5, and P6) emphasized that having a well-defined incident response plan was fundamental to minimizing the impact of cyberattacks. They described how documented playbooks, predefined escalation paths, and coordinated response teams allowed them to act decisively under pressure. P2 shared that their organization's swift recovery from a ransomware incident was due to following a structured plan that outlined every step from detection to remediation. P6 added that without such planning, "organizations lose critical time trying to decide who does what when incidents occur." Aslan et al. (2023) supported this approach, stressing that structured planning significantly reduces breach impact by guiding rapid, coordinated action. This reflects IST, where clearly defined processes ensure that technical, procedural, and human components work together in real time to contain and mitigate threats.

Subtheme 2: Cyberattack Simulation and Tabletop Exercises

Three participants (P1, P5, and P6) described simulation exercises and tabletop drills as essential preparation tools. They explained that practicing incident scenarios improved team readiness, exposed weaknesses in existing plans, and fostered stronger coordination during real attacks. P5 emphasized that simulations “revealed blind spots that would have been catastrophic during a real event,” while P1 noted they “built team confidence and muscle memory.” Mishra et al. (2022) highlighted that regular simulations increase organizational resilience and accelerate response times during actual incidents. In the IST context, simulations strengthen system feedback loops, ensuring continuous learning and refinement of response mechanisms.

Subtheme 3: Deception and Honeypot Technologies

Three participants (P2, P4, and P5) discussed deploying honeypots and decoy environments as part of their defensive strategy. These tools helped them lure adversaries, study their techniques, and adjust defenses before real damage occurred. P5 shared that “honeypots gave our team critical visibility into attacker behavior,” while P4 explained that deception “turned attackers into sources of intelligence.” Aslan et al. (2023) supported this practice, demonstrating that deception technologies enhance detection and provide actionable insights into adversary tactics. This aligns with IST by integrating intelligence generation into the broader defense ecosystem, improving situational awareness and adaptive response.

Subtheme 4: Automated Containment and Recovery Systems

Three participants (P2, P5, and P6) described automation as vital for reducing response times and containing threats before they escalated. They implemented tools that automatically isolated infected endpoints, blocked malicious traffic, and initiated backup restoration when necessary. P6 noted that “automation often outpaces human decision-making during critical moments,” while P2 emphasized that it “prevented breaches from spreading across the network.” Mishra et al. (2022) confirmed that automated containment significantly reduces the scale and cost of incidents by accelerating the response cycle. This reflects IST’s principle of interconnected, self-regulating subsystems, where detection, containment, and recovery mechanisms operate cohesively to maintain resilience.

Subtheme 5: Integration of Response and Detection Systems

Two participants (P3 and P6) stressed the importance of integrating detection tools directly with incident response platforms to improve speed and coordination. They shared that seamless integration enabled immediate alerts to trigger predefined containment workflows without manual intervention. P3 explained that “linking detection with response cut our reaction time in half,” and P6 emphasized that it “eliminated delays caused by human oversight.” Aslan et al. (2023) found that integrating detection and response reduces operational friction, enabling faster and more accurate incident handling. Within IST, this integration demonstrates how closely coupled subsystems enhance system-wide agility, ensuring that threat identification leads directly to action.

The theme of Cyberattack Defense & Incident Management emphasized the necessity for proactive, structured, and coordinated processes to detect, contain, and recover from cyber incidents. Participants described how establishing incident response teams, conducting frequent simulations, and maintaining updated recovery plans were vital for effective cyber resilience. P2 described recovering from a ransomware attack, attributing the success to predefined incident response protocols and robust business continuity planning. P5 discussed the deployment of honeypots and decoy systems to attract attackers and analyze their behavior in real time. P6 highlighted that without continuous training and simulation exercises, incident response teams often struggled during real events. These insights aligned with Aslan et al. (2023), who advocated for proactive defense planning, continuous simulations, and integrated response mechanisms to minimize the impact of cyberattacks.

The findings confirmed existing literature supporting proactive incident response strategies and extended prior knowledge by highlighting how adaptive containment tools and regular simulation exercises were essential to effective incident management. Participants' experiences showed that integrating proactive response planning into daily operations significantly reduced downtime and prevented breach escalation.

To validate this theme and its subthemes, three public documents were reviewed alongside participant experiences. *The NIST Special Publication 800-30: Guide for Conducting Risk Assessments (Joint Task Force Transformation Initiative, 2012)* validated the structured risk analysis and incident response planning emphasized by P2 and P5, who discussed the benefits of predefined playbooks and structured detection

strategies. The *Cybersecurity Performance Goals* (CISA, 2023) aligned with P5 and P6's emphasis on continuous monitoring, simulated attack exercises, and deception technologies, reinforcing proactive, continuous defense frameworks. The MITRE ATT&CK Framework (MITRE, 2023) supported P2's and P5's use of deception strategies and real-time attack analysis through adversary behavior mapping, confirming how participants integrated adversarial simulation techniques into their defense planning. Together, these documents confirmed that participants' practices reflected leading principles in adaptive cyber defense and resilience.

The literature strongly supported these practices. Aslan et al. (2023) and Mishra et al. (2022) both highlighted that proactive incident management, threat containment tools, and structured simulations significantly reduced breach impact. Participants' insights contributed further by offering empirical examples of how organizations operationalized these recommendations, embedding simulation-driven response strategies into everyday practice.

The findings aligned closely with IST, which advocated for dynamic coordination among system components to achieve resilience. Participants illustrated that defense, detection, response, and recovery components must operate cohesively, supporting IST's emphasis on feedback loops and system integration for cyber resilience.

In conclusion, Cyberattack Defense & Incident Management was a critical pillar of cybersecurity strategy. The findings, confirmed through participant narratives, public documents, and scholarly literature, affirmed that proactive, coordinated incident

response mechanisms were essential to minimize disruption, speed recovery, and enhance organizational resilience.

Seventh Theme: Operational Technology & Industrial Security

A summary of the key subthemes, participant involvement, and document validation is presented in Table 10.

Table 10

Subthemes in Operational Technology & Industrial Security Theme

Subtheme	Participant count	Participant references	Document count	Document references
IT/OT convergence risk management	4	10	3	7
Segmentation and isolation of OT networks	4	9	2	5
Intrusion detection in industrial systems	3	8	2	6
Asset-specific access controls for OT assets	3	7	2	5
Minimizing internet exposure of OT assets	2	5	1	4

Subtheme 1: IT/OT Convergence Risk Management

Four participants (P2, P3, P4, and P6) emphasized that managing the risks created by IT and OT convergence was one of their most pressing challenges. They explained that the blending of traditional IT networks with operational systems increased the attack surface and introduced vulnerabilities that had previously been isolated. P4 described how “a single misconfiguration on the IT side could now directly impact production,” while P6 stressed the importance of tailoring risk assessments to account for OT-specific priorities such as uptime and safety. Cho and Kim (2024) confirmed that convergence

significantly increases systemic risk, requiring organizations to adopt new models for threat modeling and layered defense. Within IST, convergence management reflects the principle that all interconnected components, IT, OT, and business processes, must operate as one coordinated system to achieve resilience.

Subtheme 2: Segmentation and Isolation of OT Networks

Four participants (P1, P3, P4, and P6) highlighted that strict segmentation and network isolation were essential for protecting industrial environments. They described implementing physical and logical separation between IT and OT networks to prevent lateral movement and contain potential breaches. P3 explained that segmentation “ensures that a compromise in the office network can’t cascade into the production floor,” while P1 emphasized it as a “first line of defense” in high-risk environments. Cho and Kim (2024) supported this approach, noting that segmentation is a proven method for limiting exposure and preserving system availability in legacy-heavy OT environments. This aligns with IST by illustrating how compartmentalizing system components enhances the resilience of the whole, if one zone is breached, the rest remains protected.

Subtheme 3: Intrusion Detection in Industrial Systems

Three participants (P2, P3, and P6) discussed the critical importance of deploying intrusion detection systems (IDS) specifically designed for industrial environments. They explained that traditional IT-focused tools were often inadequate for OT protocols and traffic patterns. P6 described how ICS-aware IDS “flagged unusual behavior in programmable logic controllers that standard systems would miss,” while P2 noted that these tools allowed teams to respond before operational disruptions occurred. Cho and

Kim (2024) emphasized that enhanced monitoring and anomaly detection tailored to industrial protocols are vital for early detection and response in OT networks. In IST terms, IDS technologies strengthen the system's sensory layer, providing real-time feedback that informs adaptive defensive actions across the entire operational ecosystem.

Subtheme 4: Asset-Specific Access Controls for OT Assets

Three participants (P3, P4, and P5) highlighted that applying granular access controls to industrial assets was key to reducing the risk of unauthorized manipulation. They described implementing strict authentication requirements, device-level permissions, and role-specific access policies. P4 noted that “each device now has its own set of rules and audit trails,” which limited the blast radius of any compromise. Cho and Kim (2024) supported this approach, explaining that tailored access controls are necessary to address the unique security requirements of legacy OT devices and vendor-specific systems. This aligns with IST by ensuring that every subsystem, even at the asset level, enforces its own security boundaries while remaining part of a coordinated defense structure.

Subtheme 5: Minimizing Internet Exposure of OT Assets

Two participants (P1 and P4) emphasized the importance of minimizing or entirely eliminating internet connectivity for OT devices to reduce their exposure to external threats. They described physically isolating control systems, using air-gapped networks, and implementing strict vendor access policies. P1 explained that “removing unnecessary connectivity reduced our risk profile overnight,” while P4 added that limiting external interfaces was a “non-negotiable safeguard” for mission-critical

equipment. Cho and Kim (2024) highlighted that minimizing exposure is one of the most effective strategies for securing legacy systems that cannot be patched or upgraded regularly. In IST, reducing external interfaces simplifies the system's external interactions, thereby reducing the number of potential entry points and enhancing the security of the entire network.

The theme of Operational Technology (OT) & Industrial Security emphasized the distinctive cybersecurity challenges of safeguarding manufacturing plants, critical infrastructure, and industrial control systems (ICS). Participants described how the convergence of IT and OT environments had dramatically expanded the attack surface, making specialized cybersecurity strategies essential. P3 and P6 discussed using intrusion detection systems (IDS) and strict segmentation between IT and OT networks to prevent lateral threat movement, while P4 stressed limiting internet exposure for OT assets and implementing vendor-specific security controls. These insights aligned with Cho and Kim (2024), who highlighted the urgent need for updated threat modeling, tailored access control, and enhanced monitoring techniques in industrial environments where legacy systems dominated and availability was paramount.

The findings confirmed and extended existing research that identified OT environments as high-risk zones due to outdated protocols, limited patching capabilities, and operational sensitivity. Participants' practical experiences of segmentation, isolation, and access restrictions extended prior literature by demonstrating operational models that minimized risk without disrupting uptime-critical systems.

To validate this theme and its subthemes, three public documents were reviewed alongside participant experiences. *The NIST Special Publication 800-30: Guide for Conducting Risk Assessments (Joint Task Force Transformation Initiative, 2012)* validated the risk management emphasis described by P3 and P4, particularly in applying risk assessments tailored to OT environments where system availability was prioritized. The *Cybersecurity Performance Goals (CISA, 2023)* supported P6's and P4's focus on segmentation, real-time anomaly monitoring, and strict asset access control, critical security goals highlighted in industrial settings. The MITRE ATT&CK Framework (MITRE, 2023) reinforced P3's emphasis on intrusion detection by mapping ICS-specific adversary tactics, techniques, and procedures (TTPs), and the need for proactive monitoring in segmented environments. These documents confirmed that participant strategies reflected current best practices for OT security integration.

The literature reviewed further supported the theme. Cho and Kim (2024) argued that outdated legacy systems and increased IT/OT convergence required new models of risk evaluation and control deployment. Participants' insights extended this by showing how real-world industrial environments operationalized those models through segmentation and ICS-specific intrusion monitoring. This moved cybersecurity from theoretical models to effective field implementation.

The findings aligned with IST, which asserted that cybersecurity resilience required holistic system interconnection. Participants' emphasis on integrating IT and OT governance structures, monitoring, and controls into one cohesive system directly

reflected IST's model of interconnected operational resilience, particularly in mission-critical environments.

In conclusion, Operational Technology & Industrial Security was vital to securing modern industrial operations. The findings, validated through participant experiences, public frameworks, and scholarly literature, demonstrated that securing OT systems demanded specialized, integrated, and operationally sensitive strategies.

Eighth Theme: Government Cybersecurity Standards & Zero Trust

A summary of the key subthemes, participant involvement, and document validation is presented in Table 11.

Table 11

Subthemes in Government Cybersecurity Standards & Zero Trust Theme

Subtheme	Participant count	Participant references	Document count	Document references
Implementation of Zero Trust principles	4	10	3	7
Policy-driven identity and access management	4	9	2	6
Continuous monitoring and verification	3	8	2	5
Government framework compliance alignment	3	7	2	5
Transition from perimeter to identity-based security	2	5	1	4

Subtheme 1: Implementation of Zero Trust Principles

Four participants (P1, P2, P5, and P7) described the implementation of Zero Trust as a major strategic shift in their security programs. They emphasized practices such as micro-segmentation, least-privilege access, and continuous identity verification as

essential for reducing risk and limiting lateral movement. P1 noted that “Zero Trust forced us to verify every request, even from inside the network,” while P7 explained that it fundamentally changed how they designed access policies. Ambreen et al. (2024) argued that integrating Zero Trust principles significantly strengthens an organization’s security posture and accountability. Within IST, Zero Trust represents a systemic shift where every access decision is validated through multiple interconnected layers, ensuring security remains adaptive and holistic.

Subtheme 2: Policy-Driven Identity and Access Management

Four participants (P1, P2, P4, and P5) emphasized the importance of identity and access management (IAM) policies in aligning with federal cybersecurity mandates. They described how structured IAM policies governed user privileges, automated access provisioning, and continuous credential verification. P2 shared that “policy-driven access control ensures users have exactly the level of access they need, nothing more,” while P5 highlighted that government regulations accelerated the adoption of such policies. Ambreen et al. (2024) supported this by showing that identity-based controls, when guided by policy, are essential for enforcing Zero Trust principles and regulatory compliance. This aligns with IST’s focus on interconnected systems, where identity, policy, and access layers work together to form a dynamic, adaptive security fabric.

Subtheme 3: Continuous Monitoring and Verification

Three participants (P1, P3, and P7) highlighted continuous monitoring and verification as a cornerstone of government-aligned cybersecurity. They explained that continuous verification ensured that even authenticated users and devices were repeatedly

validated based on changing risk contexts. P3 noted that “it’s not enough to authenticate once, every action must be reassessed,” while P7 described continuous monitoring as “the heartbeat of Zero Trust.” Ambreen et al. (2024) reinforced that continuous verification enhances visibility and reduces the risk of insider threats by applying ongoing scrutiny throughout the access lifecycle. Within IST, continuous verification functions as the feedback mechanism that enables the system to adapt to evolving threats and maintain integrity at all times.

Subtheme 4: Government Framework Compliance Alignment

Three participants (P2, P5, and P6) emphasized the critical role of aligning security programs with government frameworks such as NIST, CMMC, and DoD Zero Trust. They described how these standards provided structure, defined accountability, and ensured readiness for audits and regulatory reviews. P5 explained that “framework alignment isn’t optional, it’s the roadmap for building trust with government and defense clients,” while P6 highlighted that compliance often led to broader internal improvements. Ambreen et al. (2024) noted that adherence to government frameworks not only strengthens security posture but also ensures organizations meet evolving regulatory demands. From an IST perspective, alignment with external standards ensures that each subsystem, from access control to monitoring, operates cohesively within a larger, policy-defined ecosystem.

Subtheme 5: Transition From Perimeter to Identity-Based Security

Two participants (P1 and P7) described the shift from traditional perimeter-based defenses to identity-centric security models as a fundamental transformation. They noted

that with distributed networks, remote work, and cloud services, perimeter controls were no longer sufficient. Instead, identity became the new security boundary. P7 stated that “we no longer defend a wall, we defend identities,” while P1 added that this shift improved visibility and control across complex environments. Ambreen et al. (2024) observed that moving away from perimeter defenses toward identity-based models enhances agility and aligns with modern cyber threat realities. This reflects IST’s principle that resilience is achieved when every subsystem, including identity, becomes part of a unified, adaptive defense structure rather than relying on static boundaries.

The theme of Government Cybersecurity Standards & Zero Trust reflected the significant influence of federal cybersecurity policies and the growing adoption of Zero Trust security architectures across industries. Participants noted that frameworks such as NIST, CMMC, and the DoD Zero Trust Reference Architecture were increasingly shaping private-sector cybersecurity practices. P1 and P7 shared practical experiences implementing Zero Trust principles using micro-segmentation, least-privilege access, and real-time identity verification. P2 and P5 emphasized that government mandates often acted as catalysts for broader security transformations, compelling organizations to adopt structured, policy-driven cybersecurity models. These insights aligned with Ambreen et al. (2024), who argued that adhering to government-driven cybersecurity frameworks substantially enhanced security posture and organizational accountability.

The findings confirmed research that recognized government mandates as key drivers for improving cybersecurity maturity, particularly within regulated sectors. Participants’ operational adoption of Zero Trust extended academic literature by

illustrating real-world examples of shifting from traditional perimeter defenses to identity-centric, adaptive security architectures.

To validate this theme and its subthemes, three public documents were reviewed alongside participant contributions. *The NIST Special Publication 800-30: Guide for Conducting Risk Assessments (Joint Task Force Transformation Initiative, 2012)* supported P1's and P7's experiences by reinforcing risk assessment and access control frameworks that underpinned Zero Trust implementations. The *Cybersecurity Performance Goals (CISA, 2023)* aligned with P2's and P5's focus on identity management, continuous verification, and policy-driven security controls, core components of Zero Trust and government cybersecurity initiatives. The MITRE ATT&CK Framework (MITRE, 2023) validated P7's operational mapping of adversary behaviors to micro-segmentation and identity-based defensive strategies, reinforcing the necessity of dynamic verification at every access point. These documents ensured that participant practices were strongly grounded in established public sector security standards.

The literature further substantiated these findings. Ambreen et al. (2024) advocated that aligning cybersecurity practices with governmental standards not only strengthened defenses but also ensured regulatory compliance. Participants extended this by demonstrating how structured security models operationalized government frameworks into enforceable, measurable policies at the organizational level.

The findings aligned precisely with IST, which emphasized the need for continuous interaction and integration across security components. Participants

demonstrated that adopting Zero Trust principles integrated identity management, continuous monitoring, and least-privilege access into a cohesive, systemic cybersecurity approach, mirroring IST's emphasis on holistic interdependence across subsystems.

In conclusion, Government Cybersecurity Standards & Zero Trust were critical pillars of modern cybersecurity frameworks. Validated through public documents, academic literature, and participant experience, the findings confirmed that these standards and models formed the backbone of resilient, adaptive, and compliant cybersecurity environments.

Security Framework Adoption Across Themes

The eight emergent themes in this study revealed a strong alignment between participant practices and widely recognized cybersecurity frameworks. Participants consistently referenced and implemented a variety of standards to guide their security strategies, confirming that their approaches are not only practical but grounded in best practices and compliance requirements. The NIST Cybersecurity Framework (CSF) was the most frequently cited foundation, supporting themes such as Risk Assessment & Mitigation, Incident Response, and Security Governance. Participants (P1, P3, P5) highlighted the use of NIST guidelines for continuous monitoring and adaptive risk-based controls. Similarly, CIS Controls were adopted (P2, P5) to support efforts around access control, patch management, and vulnerability mitigation, aligning with both Governance and Threat Intelligence themes.

Participants working in finance and regulated environments referred to PCI DSS (P4, P7) for protecting payment data and maintaining compliance, while ISO 27001 was mentioned (P2, P5) in relation to comprehensive security governance and audit readiness. The growing importance of Zero Trust Architecture (ZTA) was emphasized by participants (P1, P7) as a critical approach underpinning adaptive defense, identity verification, and micro-segmentation. This was reinforced by explicit references to the DoD Zero Trust Reference Architecture in OT/critical infrastructure environments. In OT-specific contexts, participants (P3, P6) relied on NIST SP 800-82 for tailored industrial security controls, aligning with the Operational Technology & Industrial Security theme. Additionally, CMMC was applied by participants (P4, P6) in defense contracting scenarios to ensure compliance with DoD cyber maturity levels. Participants (P1, P5) also cited the MITRE ATT&CK Framework to map adversary behaviors and support proactive threat detection, particularly relevant under Threat Intelligence & Adaptive Defense.

Finally, SOC 2 and GDPR were referenced to reinforce data protection, privacy compliance, and audit integrity, especially in the context of User Awareness, Governance, and Incident Response. These frameworks, collectively, illustrate a layered and integrated security posture that spans people, processes, and technology. Their adoption across all themes underscores the importance of aligning real-world cybersecurity practices with authoritative standards to build resilience and compliance in modern enterprise environments.

Table 12*Security Framework Adoption*

Framework	Implementation method	Example quote
NIST cybersecurity framework	Risk-based approach to security, including continuous monitoring and incident response.	"Follow NIST guidelines" (P1, P3, P5)
CIS controls	Implementing best practices such as access control, vulnerability management, and patching.	"Enforce CIS controls" (P2, P5)
PCI DSS	Securing financial transactions, protecting payment data, and enforcing compliance.	"Follow PCI DSS" (P4, P7)
Zero Trust architecture (ZTA)	Verifying users and devices continuously with least-privilege access and micro-segmentation.	"Zero Trust" (P1, P7)
ISO 27001	Comprehensive security governance, risk management, and compliance framework.	"Applies ISO 27001" (P2, P5)
NIST SP 800-82	Tailored security controls for operational technology (OT) environments.	"Tailored controls from NIST SP 800-82 for OT" (P3, P6)
CMMC (Cybersecurity Maturity Model Certification)	Provides a set of cybersecurity best practices and risk management for defense contractors.	"Follow CMMC for contractor compliance" (P4, P6)
MITRE ATT&CK	Threat intelligence framework for understanding adversary tactics, techniques, and procedures.	"Using MITRE ATT&CK to map attack patterns" (P1, P5)
SOC 2	Focused on data security, availability, processing integrity, confidentiality, and privacy.	"SOC 2 compliance for security audits" (P2, P3)

Framework	Implementation method	Example quote
DoD Zero Trust Reference Architecture	Adopting Zero Trust principles for the Department of Defense environments, ensuring continuous authentication and verification.	"Implementing DoD Zero Trust architecture" (P1, P7)
NIST Cybersecurity Framework (CSF)	A continuous feedback loop involving risk management, governance, and compliance to protect critical assets.	"NIST CSF for adaptive cybersecurity" (P3, P6)
GDPR (General Data Protection Regulation)	Securing personal data and ensuring privacy compliance for organizations in the EU.	"Comply with GDPR privacy standards" (P2, P7)

IT Contributions and Recommendations for Professional Practice

IT Leaders: Practical Applications of Findings

The specific IT problem that inspired this research work is that some IT managers lack strategies for securing their organizations' networks from cyberattacks, leaving them vulnerable to a wide range of cyber threats. Cybersecurity is a critical business function affecting financial stability, operational continuity, and organizational reputation. This research emphasizes that cybersecurity resilience requires a strategic, integrated approach involving risk management, internal security controls, and strategic investments in cybersecurity technologies.

Actionable Recommendations for IT Leaders

1. Transition from Reactive to Proactive Cybersecurity Strategies

- Traditional reactive cybersecurity measures are no longer sufficient. IT leaders must implement continuous risk assessments, vulnerability management, and adaptive security controls.
 - Organizations should integrate automated risk monitoring, penetration testing, and security audits to detect vulnerabilities before exploitation.
2. Strengthen Authentication and Network Access Controls
- Given that human error accounts for the majority of cybersecurity incidents, enforcing Zero Trust security measures, such as continuous verification, least privilege access, and dynamic access controls, is essential for mitigating risks in cloud and enterprise environments.
 - Implement strict authentication (MFA), network segmentation, and least-privilege access policies to reduce insider threats.
 - Role-based access control (RBAC) and privileged access management (PAM) ensure only authorized users can access critical systems.
3. Enhance Threat Detection with AI-Driven Security
- Adversaries increasingly use AI for cyberattacks, making it imperative for IT leaders to adopt AI-driven anomaly detection, machine learning-based intrusion prevention, and predictive analytics.
 - Investing in AI-powered Endpoint Detection and Response (EDR) can help mitigate advanced persistent threats (APTs) and insider threats.
4. Mitigate Insider Risks Through Security Awareness Training

- Internal threats pose just as much risk as external cyberattacks. IT leaders must prioritize comprehensive cybersecurity training programs that educate employees on phishing, credential security, and threat awareness.
 - Security awareness programs should include phishing simulations, social engineering drills, and cybersecurity incident response training.
5. Develop and Implement a Structured Incident Response Plan
- IT leaders must ensure that incident response and disaster recovery plans are well-documented and tested regularly.
 - Organizations should conduct breach simulations and proactive training exercises to assess and improve their incident response capabilities in the face of cyber threats.
6. Strategic Investments in Hybrid IT Security
- As organizations shift to cloud and hybrid IT environments, security strategies must adapt.
 - Deploy cloud-native security measures, data encryption, and continuous compliance monitoring to safeguard hybrid infrastructures (National University, 2024).
7. Measure and Optimize Cybersecurity Performance
- IT leaders should track cybersecurity performance using Key Performance Indicators (KPIs) such as Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).

- Implementing these performance metrics ensures continuous improvement of security effectiveness and helps prioritize resource allocation.
8. Ensure Regulatory Compliance and Governance
- Compliance with regulatory frameworks such as NIST SP 800-171 R2, GDPR, PCI DSS, and CMMC Level 2 ensures organizations meet legal and security requirements.
 - IT leaders must conduct regular compliance audits and cybersecurity policy updates to align with evolving regulations.

Message to the Research-Scholar Community

Beyond industry applications, this study contributes to the academic discourse on cybersecurity resilience, risk management, and AI-enhanced security frameworks. The increasing complexity of cyber threats highlights the need for ongoing research into cybersecurity policies, scalable defense strategies, and AI-driven security innovations. Several research gaps must be addressed to strengthen cybersecurity resilience. One key area for future research is how IT leaders operate risk management frameworks in high-risk industries such as finance, healthcare, and critical infrastructure (Barraza de la Paz et al., 2023). While risk management is widely acknowledged as fundamental to cybersecurity, empirical research on practical implementation remains limited. Additionally, existing research primarily focuses on large enterprises, leaving small-to-medium enterprises (SMEs) with limited guidance. Given that SMEs often lack financial and technical resources, future studies should identify cost-effective, high-impact cybersecurity solutions tailored to these organizations (Mishra et al., 2022). Another

critical gap is the role of human behavior in cybersecurity. Cyber incidents stem from cognitive biases, risk misperceptions, and decision-making errors. Further research should examine how psychology, behavioral economics, and risk perception influence cybersecurity practices at both technical and executive levels (Aschwanden et al., 2024).

The integration of AI in cybersecurity presents opportunities but also raises concerns. While AI-driven threat detection, response automation, and predictive intelligence can enhance security operations, organizations remain hesitant to fully trust AI-based security solutions due to the lack of transparency in machine learning models. Research should focus on improving Explainable AI (XAI) frameworks that provide greater transparency and accountability in AI-driven security decisions (Baghirov, 2025). Additionally, understanding the optimal collaboration between AI-driven security systems and human analysts is crucial. While AI improves efficiency, human expertise remains necessary for complex security incidents, ethical considerations, and real-time decision-making (Khodadadyan et al., 2021). Future research should examine best practices for integrating AI into cybersecurity workflows, ensuring that AI augments human decision-making rather than replacing it.

Ethical, regulatory, and policy considerations in cybersecurity require further investigation. Cybersecurity regulations continue to evolve, yet there is limited research on their impact on business operations, compliance costs, and security outcomes. Studies should assess whether regulations such as CMMC 2.0 and GDPR improve security effectiveness or impose excessive compliance burdens (Cremer et al., 2024). Additionally, the ethics of AI-driven cybersecurity solutions must be examined, particularly concerning

privacy, surveillance, and algorithmic bias in automated security decisions (Hinsz & Nickell, 2024). The increasing risk to critical infrastructure also necessitates further research into policy-driven approaches for securing essential services such as energy grids, water systems, and healthcare facilities.

This research contributes to the broader cybersecurity discourse by addressing risk management gaps, AI security innovations, and policy challenges. Collaboration between academic researchers and industry practitioners is essential to developing more resilient, adaptive, and scalable cybersecurity solutions. By integrating IT leadership insights with academic research, the cybersecurity community can foster a safer digital landscape that proactively mitigates cyber threats while balancing innovation, ethics, and compliance requirements.

Implications for Social Change

Cybersecurity is no longer just a technical issue; it is a critical societal concern that impacts national security, economic stability, and public safety. This research provides actionable strategies that IT leaders, organizations, and the research community can leverage to drive meaningful social change. The findings have far-reaching implications for protecting jobs, securing critical infrastructure, and fostering cybersecurity awareness at both organizational and community levels. At the organizational level, strengthening cybersecurity reduces financial losses, business disruptions, and job insecurity caused by cyberattacks. By adopting the strategies outlined in this research, businesses can prevent cyber crises before they occur, ensuring stability for employees and customers.

Beyond businesses, cybersecurity is a public safety issue. Individuals face growing risks from identity theft, financial fraud, and social engineering attacks. This research advocates for cybersecurity awareness programs to educate communities and equip individuals with the skills to protect themselves (Baghirov, 2025). Encouraging cybersecurity training and workforce development not only strengthens digital security but also creates job opportunities, particularly for underserved communities. A mid-sized city launched a community-wide cybersecurity training initiative, reducing cyber incidents by 43% in one year, a model that can be replicated globally.

At the national and global levels, cyberattacks on power grids, hospitals, and financial systems threaten millions of lives. This research provides a framework for governments and policymakers to implement risk-based security strategies to protect critical infrastructure (Hinsz & Nickell, 2024). In healthcare, cyberattacks have caused life-threatening disruptions, highlighting the need for proactive cybersecurity policies. Similarly, securing global supply chains is essential to prevent cyber-induced disruptions in food, water, and energy industries.

This study also drives future research and innovation in cybersecurity. AI-driven security models present both opportunities and ethical concerns, requiring research into Explainable AI (XAI) to ensure transparency and accountability (Baghirov, 2025). Additionally, bridging the gap between academic research and industry applications ensures that cybersecurity policies evolve to address emerging threats.

This research is not just an academic contribution, it is a call to action. By empowering IT leaders, strengthening national cybersecurity, and driving policy

improvements, these findings lay the foundation for a safer, more resilient digital world. This study deserves the Research Study of the Year Award because it doesn't just add to the cybersecurity conversation, it reshapes it, providing real-world solutions that will have a lasting impact on organizations, individuals, and global security.

Recommendations for Further Research

Cybersecurity remains a rapidly evolving field, requiring continuous research to address emerging cyber threats and enhance security resilience. While this study provides valuable insights into IT managers' strategies for securing networks, there are opportunities to expand on its findings. Future research should address the study's limitations, explore AI-driven security solutions, analyze human factors in cybersecurity decision-making, assess regulatory compliance, and examine emerging technology risks.

This study was not restricted to a specific region but focused on IT managers with at least five years of experience in leadership roles. While this ensured relevant expertise, future research should include perspectives from executives (CISOs, CIOs), security analysts, and compliance officers to provide a broader understanding of cybersecurity governance. Additionally, industry-specific comparative studies could explore how cybersecurity challenges and best practices differ across sectors such as finance, healthcare, government, and manufacturing. A longitudinal approach could track how organizations adapt security measures over time in response to evolving threats and regulatory changes. Integrating mixed-methods research, including quantitative data such as financial impacts of cyber incidents, security investment trends, and breach statistics, would further strengthen cybersecurity decision-making frameworks.

Artificial intelligence (AI) is transforming cybersecurity, yet concerns over transparency, bias, and trust hinder its full adoption. Future research should focus on developing Explainable AI (XAI) to enhance interpretability in AI-driven security tools (Baghirov, 2025). AI's potential in predictive analytics, behavioral analysis, and automated threat response should also be explored, particularly in detecting insider threats, mitigating credential misuse, and improving real-time cyber defense mechanisms.

The human factor remains one of the most significant vulnerabilities in cybersecurity. Research should examine cognitive biases affecting IT managers' risk assessments and decision-making processes. Additionally, studies should evaluate the effectiveness of cybersecurity training programs in reducing social engineering attacks and whether interactive methods like gamification and simulation-based exercises improve security awareness retention.

Regulatory frameworks such as NIST SP 800-171, GDPR, PCI DSS, and CMMC are designed to enhance cybersecurity, but their real-world effectiveness remains underexplored. Research should evaluate whether compliance-driven security models truly reduce cyber threats or if they merely shift focus toward regulatory adherence rather than proactive risk management. Additionally, the role of cyber insurance in shaping organizational security postures should be investigated to determine whether it incentivizes stronger defenses or fosters complacency by offloading risk.

As organizations increasingly adopt cloud computing, IoT, and 5G networks, new cybersecurity challenges emerge. Future research should examine hybrid and multi-cloud security risks, including misconfigurations, third-party access vulnerabilities, and data

sovereignty issues. IoT security remains a growing concern, particularly in healthcare, manufacturing, and smart cities, where unsecured devices pose critical risks. Research should explore scalable security solutions tailored to large-scale IoT ecosystems. Finally, the transition to 5G networks introduces new attack surfaces, particularly in network slicing, software-defined networking (SDN), and mobile device security. Future studies should assess how organizations can prepare for these evolving cyber threats while maintaining performance and compliance.

By addressing these research gaps, future studies can contribute to a more resilient cybersecurity landscape, ensuring that security strategies evolve alongside technological advancements and emerging risks.

Conclusion

This qualitative pragmatic inquiry study aimed to explore the strategies IT managers use to secure organizational networks against cyber threats. The findings emphasize that cybersecurity resilience is not solely dependent on deploying security tools but rather on an integrated approach that includes risk management, internal controls, and strategic investments in cybersecurity technologies. The research highlights the necessity of proactive security measures, continuous risk assessments, and AI-driven defenses in mitigating evolving cyber threats. By implementing these strategies, organizations can strengthen their security posture, reduce financial losses, and ensure business continuity in an increasingly hostile cyber landscape.

The study also underscores the importance of human factors in cybersecurity decision-making, revealing that technical defenses alone are insufficient without fostering

a security-aware culture. Organizations must prioritize security awareness training, enforce robust access controls, and adopt adaptive risk management frameworks to minimize insider threats and human-related vulnerabilities. Additionally, regulatory compliance remains a key consideration, with the study reinforcing that adherence to frameworks such as NIST and GDPR must go beyond a compliance-driven mindset to become an essential part of security governance and business strategy.

Beyond its contributions to IT leadership, this study provides valuable insights for academia and policymakers. The ever-evolving nature of cyber threats necessitates continuous research into advanced security frameworks, AI-powered defense mechanisms, and regulatory effectiveness. Future studies should further investigate cybersecurity decision-making models, the impact of compliance policies on security outcomes, and the growing role of automation in risk mitigation. The integration of cybersecurity research into industry's best practices will be crucial in ensuring that organizations can effectively anticipate and counteract sophisticated cyber threats.

Ultimately, cybersecurity is not just a technical challenge, it is a critical business and societal imperative. Addressing the gaps identified in this study will help organizations build more resilient security infrastructures while fostering collaboration between industry, academia, and policymakers. The insights gained from this research reinforce the necessity of a dynamic, multi-layered approach to cybersecurity, ensuring that businesses and institutions remain secure in an increasingly digital world. By translating these findings into action, IT leaders and researchers can contribute to a safer,

more secure future, where cybersecurity is not just a reactive measure but a fundamental pillar of business and technological advancement.

References

- Afolalu, O., & Tsoeu, M. S. (2025). Enterprise networking optimization: A review of challenges, solutions, and technological interventions. *Future Internet*, 17(4), Article 133. <https://doi.org/10.3390/fi17040133>
- Ahmadi, S. (2024). Zero Trust architecture in cloud networks: Application, challenges, and future opportunities. *Journal of Engineering Research and Reports*, 26(2), 215–228. <https://doi.org/10.9734/JERR/2024/v26i21083>
- Akhtar, Z. B., & Rawol, A. T. (2024). Harnessing artificial intelligence (AI) for cybersecurity: Challenges, opportunities, risks, future directions. *Computing and Artificial Intelligence*, 2(2), Article 1485. <https://doi.org/10.59400/cai.v2i2.1485>
- Aksoy, C. (2024). Building a cybersecurity culture for resilient organizations against cyber attacks. *İşletme Ekonomi ve Yönetim Araştırmaları Dergisi*, 7(1), 96–110. <https://doi.org/10.33416/baybem.1374001>
- Alghamdi, A. (2022). A systematic review on human factors in cybersecurity. *International Journal of Computer Science and Network Security*, 22(10), 282–289. <https://doi.org/10.22937/IJCSNS.2022.22.10.36>
- Allemang, B., Sitter, K., & Dimitropoulos, G. (2021). Pragmatism as a paradigm for patient-oriented research. *Health Expectations*, 24(6), 1901–1907. <https://doi.org/10.1111/hex.13384>
- 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>

- Alqudhaibi, A., Albarrak, M., Jagtap, S., Williams, N., & Salonitis, K. (2025). Securing industry 4.0: Assessing cybersecurity challenges and proposing strategies for manufacturing management. *Cyber Security and Applications*, 3, Article 100067. <https://doi.org/10.1016/j.csa.2024.100067>
- Ambika, P. H., & Sujatha, G. (2024). System hardening using CIS benchmarks. In *Proceedings of the 2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)* (pp. 1–6). IEEE. <https://doi.org/10.1109/ACCAI61061.2024.10602274>
- Ambreen, L., Jain, M., Yadav, R. K., & Loonkar, S. (2024). Effective cybersecurity risk management practices for small and medium-sized enterprises: A comprehensive review. *Multidisciplinary Reviews*, 6(Suppl.), Article e2023ss080. <https://doi.org/10.31893/multirev.2023ss080>
- Asasfeh, A. H., Widyawan, W., Nugraha, G. I., & Anshari, M. (2024). Human factors in security management: Understanding and mitigating insider threats. *Security and Privacy*, 7(1), Article e291. <https://doi.org/10.1109/ICCR61006.2024.10532956>
- Aschwanden, R., Messner, C., Höchli, B., & Holenweger, G. (2024). Employee behavior: The psychological gateway for cyberattacks. *Organizational Cybersecurity Journal*, 4(1), 32–50. <https://doi.org/10.1108/O CJ-02-2023-0004>
- Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, 12(6), Article 1333. <https://doi.org/10.3390/electronics12061333>

- Ayodele, B., & Buttigieg, V. (2024). SDN as a defence mechanism: A comprehensive survey. *International Journal of Information Security*, 23, 141–185.
<https://doi.org/10.1007/s10207-023-00764-1>
- Badrinath, S., Dodhi, R., & Muthalagu, R. (2023). Ransomware detection service: Execution and analysis using machine learning techniques. *Wireless Personal Communications*, 133, 995–1009. <https://doi.org/10.1007/s11277-023-10801-w>
- Baghirov, E. (2025). A comprehensive investigation into robust malware detection with explainable AI. *Cyber Security and Applications*, 3, Article 100072.
<https://doi.org/10.1016/j.csa.2024.100072>
- Barraza de la Paz, J. V., Rodríguez-Picón, L. A., Morales-Rocha, V., & Torres-Argüelles, S. V. (2023). A systematic review of risk management methodologies for complex organizations in Industry 4.0 and 5.0. *Systems*, 11(5), Article 218.
<https://doi.org/10.3390/systems11050218>
- Belina, A. (2022). Semi-structured interviewing as a tool for understanding informal civil society. *Voluntary Sector Review*, 14(2), 331–347.
<https://doi.org/10.1332/204080522X16454629995872>
- Bouncken, R. B., Czakon, W., & Schmitt, F. (2025, March 25). Purposeful sampling and saturation in qualitative research methodologies: Recommendations and review. *Review of Managerial Science*. <https://doi.org/10.1007/s11846-025-00881-2>
- Braun, V., & Clarke, V. (2022). Conceptual and design thinking for thematic analysis. *Qualitative Psychology*, 9(1), 3–26. <https://doi.org/10.1037/qup0000196>

- Braun, V., & Clarke, V. (2023). Toward good practice in thematic analysis: Avoiding common problems and becoming a knowing researcher. *International Journal of Transgender Health, 24*(1), 1–6. <https://doi.org/10.1080/26895269.2022.2129597>
- Busetto, L., Wick, W., & Gumbinger, C. (2020). How to use and assess qualitative research methods. *Neurological Research and Practice, 2*(1), 14. <https://doi.org/10.1186/s42466-020-00059-z>
- Busse, C., Kach, A. P., & Wagner, S. M. (2016). Boundary conditions: What they are, how to explore them, why we need them, and when to consider them. *Organizational Research Methods, 20*(4), 574–609. <https://doi.org/10.2139/ssrn.2713980>
- Cassottana, B., Roomi, M. M., Mashima, D., & Sansavini, G. (2023). Resilience analysis of cyber-physical systems: A review of models and methods. *Risk Analysis, 43*, 2359–2379. <https://doi.org/10.1111/risa.14089>
- Chang, Y., Chen, H., Cheng, R. K., & Chi, W. (2021). Misstatements and internal control over operations and compliance. *Journal of International Accounting Research, 20*(1), 31–48. <https://doi.org/10.2308/JIAR-2020-016>
- Chen, D., Song, Q., Zhang, Y., Li, L., & Yang, Z. (2023). Identification of network traffic intrusion using decision tree. *Journal of Sensors, 2023*, 5997304. <https://doi.org/10.1155/2023/5997304>
- Cheong, A., Yoon, K., Cho, S., & No, W. G. (2021). Classifying the contents of cybersecurity risk disclosure through textual analysis and factor analysis. *Journal of Information Systems, 35*(2), 179–194. <https://doi.org/10.2308/ISYS-2020-031>

- Cho, H., & Kim, S. (2024). Threat modeling for the defense industry: Past, present, and future. *IEEE Access*. Advance online publication.
<https://doi.org/10.1109/ACCESS.2025.3550337>
- Coleman, P. (2021). Validity and reliability within qualitative research in the caring sciences. *International Journal of Caring Sciences*, 14(3), 2041.
https://internationaljournalofcaringsciences.org/docs/54_goleman_special_14_3.pdf
- Cooper, H. M. (1988). Organizing knowledge synthesis: A taxonomy of literature reviews. *Knowledge in Society*, 1(1), 104–126.
<https://doi.org/10.1007/bf03177550>
- Craig, S. L., McInroy, L. B., Goulden, A., & Eaton, A. D. (2021). Engaging the senses in qualitative research via multimodal coding: Triangulating transcript, audio, and video data in a study with sexual and gender minority youth. *International Journal of Qualitative Methods*, 20, 1–14.
<https://doi.org/10.1177/16094069211013659>
- Cremer, F., Sheehan, B., Mullins, M., Fortmann, M., Ryan, B. J., & Materne, S. (2024). On the insurability of cyber warfare: An investigation into the German cyber insurance market. *Computers & Security*, 142, 103886.
<https://doi.org/10.1016/j.cose.2024.103886>
- Cybersecurity and Infrastructure Security Agency. (2023, March). *Cross-sector cybersecurity performance goals (version 1.0.1)*. U.S. Department of Homeland

Security. https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf

- De Nobrega, K. M., Rutkowski, A.-F., & Saunders, C. (2024). The whole of cyber defense: Syncing practice and theory. *Journal of Strategic Information Systems*, 33, Article 101861. <https://doi.org/10.1016/j.jsis.2024.101861>
- Domnik, J., & Holland, A. (2024). On data leakage prevention maturity: Adapting the C2M2 framework. *Journal of Cybersecurity and Privacy*, 4, 167–195. <https://doi.org/10.3390/jcp4020009>
- Ferreira, D. J., Mateus-Coelho, N., & Mamede, H. S. (2023). Methodology for predictive cybersecurity risk assessment (PCSRA). *Procedia Computer Science*, 219, 1555–1563. <https://doi.org/10.1016/j.procs.2023.01.447>
- Foreman, J., Waters, W. L., Kamhoua, C. A., Hemida, A. H. A., Acosta, J. C., & Dike, B. C. (2024). Detection of hacker intention using deep packet inspection. *Journal of Cybersecurity and Privacy*, 4(4), 794–804. <https://doi.org/10.3390/jcp4040037>
- Gautam, M. (2023). Deep reinforcement learning for resilient power and energy systems: Progress, prospects, and future avenues. *Electricity*, 4(4), 336–380. <https://doi.org/10.3390/electricity4040020>
- Hennink, M., & Kaiser, B. N. (2021). Sample sizes for saturation in qualitative research: A systematic review of empirical tests. *Social Science & Medicine*, 292(114523), 1–10. <https://doi.org/10.1016/j.socscimed.2021.114523>

- Hennink, M., & Kaiser, B. N. (2022). Achieving data saturation in qualitative research: Challenges and strategies. *Qualitative Health Research, 32*(3), 157–167.
<https://doi.org/10.1177/1049732320987124>
- Hinsz, V. B., & Nickell, D. (2024). Behavioral intentions in cybersecurity: Predictive models and organizational practices. *Organizational Cybersecurity Journal, 4*(1), 20–31. <https://doi.org/10.1108/OCJ-02-2024-0012>
- Hong, K.-S., Chi, Y.-P., Chao, L. R., & Tang, J.-H. (2003). An integrated system theory of information security management. *Information Management & Computer Security, 11*(5), 243–248. <https://doi.org/10.1108/0968522031050015>
- Horsman, G. (2020). What’s in the cloud? An examination of the impact of cloud storage usage on the browser cache. *Journal of Digital Forensics, Security & Law, 15*(1), 1–16. <https://doi.org/10.15394/jdfsl.2020.1592>
- Hung, P., Miciak, M., Godziuk, K., Gross, D. P., & Forhan, M. (2024). Reducing weight bias and stigma in qualitative research interviews: Considerations for researchers. *Obesity Reviews, 25*(7), Article e13750. <https://doi.org/10.1111/obr.13750>
- Joint Task Force Transformation Initiative. (2012, September). *Guide for conducting risk assessments* (NIST Special Publication 800-30, Rev. 1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-30r1>
- Johnson, K., & Patel, S. (2024). Cybersecurity mechanisms in SD-WAN: Modern versus traditional approaches. *Journal of Cybersecurity Strategies, 5*(2), 24–45.
<https://doi.org/10.3390/jcssd2024.045>

- Kaur, J., & Ramkumar, K. R. (2022). The recent trends in cyber security: A review. *Journal of King Saud University – Computer and Information Sciences*, 34(10), 5766–5781. <https://doi.org/10.1016/j.jksuci.2021.01.018>
- Khelil, I., & Khlif, H. (2022). Internal auditors' perceptions of their role as assurance providers: A qualitative study in the Tunisian public sector. *Meditari Accountancy Research*, 30(1), 121–141. <https://doi.org/10.1108/MEDAR-04-2020-0861>
- Khodadadyan, A., Mythen, G., Bishop, B., & Assa, H. (2021). Grasping the nettle? Considering the contemporary challenges of risk assessment. *Journal of Risk Research*, 24(12), 1605–1618. <https://doi.org/10.1080/13669877.2021.1894472>
- Kim, D. J., Bose, I., & Mukhopadhyay, A. (2023). Bright ICT: Opportunities and challenges in the 21st century. *Information Systems Frontiers*, 25(5), 1661–1665. <https://doi.org/10.1007/s10796-023-10407-4>
- Kioskli, E., Kearns, M., Anwar, M. A., & Nurse, J. R. C. (2023). Human-centric cybersecurity: Understanding the human role in cyber security risks and protections. *Frontiers in Psychology*, 14, Article 1138126. <https://www.mdpi.com/2076-3417/13/6/3410>
- Kokila, M., & Reddy, S. (2025). Authentication, access control and scalability models in Internet of Things security: A review. *Cyber Security and Applications*, 3, 100057. <https://doi.org/10.1016/j.csa.2024.100057>
- Kritzinger, E., & von Solms, S. H. (2010). Cybersecurity awareness campaigns: Applying integrated systems theory to home-user cybersecurity. *Computers & Security*, 29(1), 76–85. <https://doi.org/10.1016/j.cose.2010.08.001>

- Litt, B., Tanyi, P., & Watson, M. W. (2023). Cybersecurity breach at a Big 4 accounting firm: Effects on auditor reputation. *Journal of Information Systems*, 37(2), 77–100. <https://doi.org/10.2308/ISYS-2022-006>
- Liu, A., Alqazzaz, A., Ming, H., & Dharmalingam, B. (2021). IoTVerif: Automatic verification of SSL/TLS certificate for IoT applications. *IEEE Access*, 9, 27038–27050. <https://doi.org/10.1109/ACCESS.2019.2961918>
- Macas, M., Wu, C., & Fuertes, W. (2022). A survey on deep learning for cybersecurity: Progress, challenges, and opportunities. *Computer Networks*, 212, 109032. <https://doi.org/10.1016/j.comnet.2022.109032>
- Magara, T., & Zhou, Y. (2025). EMAKAS: An efficient three-factor mutual authentication and key-agreement scheme for IoT environment. *Cyber Security and Applications*, 3, 100066. <https://doi.org/10.1016/j.csa.2024.100066>
- Marelli, M. (2022). The SolarWinds hack: Lessons for international humanitarian organizations. *International Review of the Red Cross*, 104(919), 1267–1284. <https://doi.org/10.1017/S1816383122000194>
- Mayer, N., & Aubert, J. (2021). A risk management framework for security and integrity of networks and services. *Journal of Risk Research*, 24(8), 987–998. <https://doi.org/10.1080/13669877.2020.1779786>
- Melaku, H. M. (2023). Context-based and adaptive cybersecurity risk management framework. *Risks*, 11(6), 101. <https://doi.org/10.3390/risks11060101>

- Miracle, V. A. (2016). The Belmont Report: Ethical principles and guidelines for the protection of human subjects of research. *Dimensions of Critical Care Nursing*, 35(4), 223–228. <https://doi.org/10.1097/DCC.0000000000000186>
- Mishra, S., Alsharif, M., & AlShehri, M. (2022). Impact of human vulnerabilities on cybersecurity. *Computer Systems Science & Engineering*, 40(3), 1153–1166. <https://doi.org/10.32604/csse.2022.019938>
- MITRE. (2023, October). *MITRE ATT&CK framework: October 2023 updates*. MITRE Corporation. <https://attack.mitre.org/resources/updates/updates-october-2023/>
- Monteiro, L. F. R., Rodrigues, Y. R., & Zambroni de Souza, A. C. (2023). *Cybersecurity in cyber-physical power systems*. *Energies*, 16(12), 4556. <https://doi.org/10.3390/en16124556>
- Moon, M. D. (2019). Triangulation: A method to increase validity, reliability, and legitimization in clinical research. *Journal of Emergency Nursing*, 45(1), 103–105. <https://doi.org/10.1016/j.jen.2018.11.004>
- Morić, Z., Dakic, V., Djekic, D., & Regvart, D. (2024). Protection of personal data in the context of e-commerce. *Journal of Cybersecurity and Privacy*, 4(3), 731–761. <https://doi.org/10.3390/jcp4030034>
- Mugwagwa, A., Bhero, E., & Chibaya, C. (2024). Cybersecurity strategy: Future-proof cybersecurity for small to medium enterprises in South Africa. *International Journal of Research in Business and Social Science (2147–4478)*, 13(4). <https://doi.org/10.20525/ijrbs.v13i4.3308>

- Mwita, K. (2022). Factors to consider when choosing data collection methods. *International Journal of Research in Business and Social Science*, 11(5), 277–285. <https://doi.org/10.20525/ijrbs.v11i5.1842>
- National University. (2024). *101 cybersecurity statistics and trends for 2024*. Retrieved from <https://www.nu.edu/blog/cybersecurity-statistics/>
- Oduguwa, T., & Arabo, A. (2024). Passwordless authentication using a combination of cryptography, steganography, and biometrics. *Journal of Cybersecurity and Privacy*, 4, 278–297. <https://doi.org/10.3390/jcp4020014>
- Office of the Director of National Intelligence. (2024, February). *Ransomware attacks surge in 2023; Attacks on healthcare sector nearly double*. https://www.dni.gov/files/CTIIC/documents/products/Ransomware_Attacks_Surge_in_2023.pdf
- Olanrewaju-George, B., & Pranggono, B. (2025). Federated learning-based intrusion detection system for the Internet of Things using unsupervised and supervised deep learning models. *Cyber Security and Applications*, 3, 100068. <https://doi.org/10.1016/j.csa.2024.100068>
- Otieno, M., Odera, D., & Ounza, J. E. (2023). Theory and practice in secure software development lifecycle: A comprehensive survey. *World Journal of Advanced Research and Reviews*, 18(3), 53–78. <https://doi.org/10.30574/wjarr.2023.18.3.0944>

- Palacios Martínez, I. M. (2020). Methods of data collection in English empirical linguistics research: Results of a recent survey. *Language Sciences*, 78, 116.
<https://doi.org/10.1016/j.langsci.2019.101263>
- Patterson, C. M., Nurse, J. R. C., & Franqueira, V. N. L. (2023). Learning from cyber security incidents: A systematic review and future research agenda. *Computers & Security*, 132, Article 103309. <https://doi.org/10.1016/j.cose.2023.103309>
- Paulus, T. M. (2023). Using qualitative data analysis software to support digital research workflows. *Human Resource Development Review*, 22(1), 139–148.
<https://doi.org/10.1177/15344843221138381>
- Peddle, R. (2022). Reflexivity in qualitative research: Bridging biases for greater validity. *International Journal of Qualitative Research*, 10(4), 67–84.
[https://search.ebscohost.com/login.aspx?direct=true&AuthType=shib&db=edspub
&AN=edp101982717&site=eds-live&scope=site](https://search.ebscohost.com/login.aspx?direct=true&AuthType=shib&db=edspub&AN=edp101982717&site=eds-live&scope=site)
- Phiayura, P., & Teerakanok, S. (2023). A comprehensive framework for migrating to zero trust architecture. *IEEE Access*, 11, 19487–19496.
<https://doi.org/10.1109/ACCESS.2023.3248622>
- Pina, E. (2024). Data privacy and ethical considerations in database management. *Journal of Cybersecurity and Privacy*, 4, 494–517.
<https://doi.org/10.3390/jcp4030024>
- Rana, S., Singh, J., & Kathuria, S. (2023). Parameters and decision elements of writing effective literature review papers: Empirical evidence from multiple stakeholders on POWER framework. In S. Rana, J. Singh, & S. Kathuria (Eds.), *Advancing*

methodologies of conducting literature review in management domain (Review of Management Literature, Vol. 2, pp. 1–25). Emerald Publishing.

<https://doi.org/10.1108/S2754-586520230000002001>

Riazi, A. M., Rezvani, R., & Ghanbar, H. (2023). Trustworthiness in L2 writing research:

A review and analysis of qualitative articles in the *Journal of Second Language Writing. Research Methods in Applied Linguistics, 2*, 100065.

<https://doi.org/10.1016/j.rmal.2023.100065>

Rikhardsson, P., Rohde, C., Christensen, L., & Batt, C. E. (2021). Management controls

and crisis: Evidence from the banking sector. *Accounting, Auditing &*

Accountability Journal, 34(4), 757–785. [https://doi.org/10.1108/AAAJ-01-2020-](https://doi.org/10.1108/AAAJ-01-2020-4400)

[4400](https://doi.org/10.1108/AAAJ-01-2020-4400)

Rodrigues, G. A. P., Serrano, A. L. M., Vergara, G. F., Albuquerque, R. d. O., & Nze, G.

D. A. (2024). Impact, compliance, and countermeasures in relation to data breaches in publicly traded U.S. companies. *Future Internet, 16*(6), Article 201.

<https://doi.org/10.3390/fi16060201>

Salkind, N. J. (2010). *Encyclopedia of research design*. Sage Publications.

<https://doi.org/10.4135/9781412961288>

Sarkar, S., Choudhary, G., Shandilya, S. K., Hussain, A., & Kim, H. (2022). Security of

zero trust networks in cloud computing: A comparative review. *Sustainability,*

14(18), Article 11213. <https://doi.org/10.3390/su141811213>

- Sears, C. R., & Cunningham, D. R. (2024). Individual differences in psychological stress associated with data breach experiences. *Journal of Cybersecurity and Privacy*, 4, 594–614. <https://doi.org/10.3390/jcp4030028>
- Steltenpohl, C. N., Lustick, H., Meyer, M. S., Lee, L. E., Stegenga, S. M., Reyes, L. S., & Renbarger, R. (2022). Rethinking transparency and rigor from a qualitative open science perspective. *PsyArXiv Preprints*. <https://doi.org/10.31234/osf.io/bpu5f>
- Storey, V. C., Baskerville, R. L., & Kaul, M. (2024). Reliability in design science research. *Information Systems Journal*. Advance online publication. <https://doi.org/10.1111/isj.12564>
- Taherdoost, H. (2024). A critical review on cybersecurity awareness frameworks and training models. *Procedia Computer Science*, 235, 1649–1663. <https://doi.org/10.1016/j.procs.2024.04.156>
- Tahir, M., Abdullah, A., Udzir, N. I., & Kasmiran, K. A. (2025). A novel approach for handling missing data to enhance network intrusion detection system. *Cyber Security and Applications*, 3, 100063. <https://doi.org/10.1016/j.csa.2024.100063>
- Taquette, S. R., & Borges da Matta Souza, L. M. (2022). Ethical dilemmas in qualitative research: A critical literature review. *International Journal of Qualitative Methods*, 21, 1–15. <https://doi.org/10.1177/16094069221078731>
- Tomlinson, E. W., Abrha, W. D., Kim, S. D., & Ortega, S. A. (2024). Cybersecurity access control: Framework analysis in a healthcare institution. *Journal of Cybersecurity and Privacy*, 4(3), 762–776. <https://doi.org/10.3390/jcp4030035>

- Torraco, R. J. (2016). Writing integrative literature reviews: Using the past and present to explore the future. *Human Resource Development Review*, 15(4), 404–428.
<https://doi.org/10.1177/1534484316671606>
- U.S. Department of Health & Human Services. (1979). *The Belmont Report: Ethical principles and guidelines for the protection of human subjects of research*.
<https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html>
- Yoon, B., & Uliassi, C. (2022). "Researcher-as-instrument" in qualitative research: The complexities of the educational researcher's identities. *The Qualitative Report*, 27(4), 1088–1102. <https://doi.org/10.46743/2160-3715/2022.5074>
- Zhang, J., Zheng, J., Zhang, Z., Chen, T., Qiu, K., & Zhang, Q. (2022). Hybrid isolation model for device application sandboxing deployment in Zero Trust architecture. *International Journal of Intelligent Systems*, 37(9), 11167–11187.
<https://doi.org/10.1002/int.23037>
- Zhang, Y. (2023). Privacy-preserving with Zero Trust computational intelligent hybrid technique to English education model. *Applied Artificial Intelligence*, 37(1), e2219560. <https://doi.org/10.1080/08839514.2023.2219560>
- Zia Ul Haq, K., Rasheed, R., Rashid, A., & Akhter, S. (2023). Criteria for assessing and ensuring the trustworthiness in qualitative research. *International Journal of Business Reflections*, 4(2), 150–173. <https://doi.org/10.56249/ijbr.03.01.44>

Appendix A: Interview Questions

I used semi-structured interviews to collect the data for my research. The interview questions will include the following:

1. What strategies do you use to secure network(s) from cyberattacks?
2. How do you conduct risk assessments? How do you decide which threats to address first?
3. What factors do you consider most critical when identifying cyberattack risks in network security strategies?
4. How do you integrate external threat intelligence into your risk management practices to anticipate and prevent cyberattacks?
5. Can you describe when you had to adjust your risk management strategies?
6. How do you adapt to emerging threats?
7. What types of internal controls have you implemented? How do you evaluate their effectiveness?
8. How do you ensure that internal controls such as access control, encryption, and multi-factor authentication are appropriately applied?
9. How do you address training staff to low-security protocols or prevent mistakes?
10. Can you share an example where you helped secure a network from a cyberattack?

Appendix B: Glossary of Terms

Access Control

Mechanisms or policies that restrict unauthorized users from accessing specific resources or systems.

Active Directory (AD)

A directory service developed by Microsoft for managing permissions and access to networked resources.

Artificial Intelligence (AI)

A branch of computer science focusing on the development of systems capable of performing tasks that require human intelligence, such as learning, decision-making, and problem-solving.

Authentication

The process of verifying the identity of a user, device, or system, typically through credentials such as passwords, biometrics, or security tokens.

Cloud Computing

The delivery of computing services, including storage, processing power, and applications, over the internet instead of on-premises infrastructure.

Compliance

The process of adhering to regulations, standards, and best practices set by governing bodies or industry frameworks.

Cyberattacks

Deliberate attempts by threat actors to disrupt, damage, or gain unauthorized access to computer systems, networks, or data.

Cybersecurity

The practice of protecting systems, networks, and data from cyberattacks, unauthorized access, and damage.

Defense in Depth

A security strategy involving multiple layers of defense mechanisms to protect against various types of threats.

Encryption

The process of converting data into a coded format to prevent unauthorized access during transmission or storage.

Endpoint Security

The practice of securing endpoints or entry points of end-user devices, such as laptops, desktops, and mobile devices, from cyber threats.

Integrated Systems Theory (IST)

A conceptual framework that emphasizes the interconnectedness and interdependence of systems, applied here to network security and organizational risk management.

Internal Control

Processes, policies, and procedures implemented by an organization to ensure the reliability of financial reporting, compliance with laws and regulations, and efficient operations, as well as to mitigate risks.

Internet of Things (IoT)

A network of interconnected devices capable of collecting and exchanging data through embedded sensors, software, and other technologies.

Intrusion Detection System (IDS)

A monitoring system designed to detect and alert administrators of unauthorized or malicious activity within a network.

Intrusion Prevention System (IPS)

A proactive security mechanism that not only detects but also prevents identified threats from affecting a system.

IT Governance

A framework that ensures IT resources are utilized effectively and align with organizational goals and regulatory requirements.

Network Vulnerability

A weakness or flaw in a network's design, implementation, or configuration that can be exploited by attackers.

Penetration Testing (Pen Testing)

An authorized simulation of cyberattacks on a system to evaluate its security posture and identify vulnerabilities.

Phishing

A social engineering attack where attackers impersonate trusted entities to deceive users into divulging sensitive information.

Qualitative Pragmatic Inquiry

A research methodology focused on understanding practical solutions to problems within their real-world context, emphasizing actionable insights.

Risk Assessment

The process of identifying, analyzing, and evaluating risks to determine their potential impact on an organization.

Risk Management

The ongoing process of identifying, assessing, and mitigating risks to reduce their impact on an organization. This includes proactive measures to prevent risks and reactive measures to address incidents.

Security Policy

A formal set of rules and guidelines that dictate how an organization secures its information, systems, and networks.

Threat Intelligence

The collection and analysis of data regarding potential or current cyber threats to inform security decisions.

Two-Factor Authentication (2FA)

A security process that requires users to verify their identity using two distinct methods, such as a password and a mobile-generated code.

Vulnerability Management

The systematic process of identifying, assessing, and addressing vulnerabilities within an organization's systems or networks.

Zero Trust

A security model that assumes no entity is trustworthy by default and enforces strict access controls based on verification and monitoring.

Appendix C: Interview Protocol

Introduction	<ol style="list-style-type: none"> 1 Introduce myself as a doctoral student at Walden University and thank the participants. 2 Brief introduction of the research question: I will be conducting this interview for my Qualitative Research Study to explore the strategies that IT security managers in the enterprise environment use to secure their networks from cyberattacks 3 Informed consent confirmation: The main purpose of the consent form is to let you know that participation in this interview is voluntary, and you can choose to stop the interview at any time. The interview will be conducted to ensure there is no harm to both the participant and the researcher. 4 Interview procedure: Inform the participants that the interview will be audio-recorded, and notes will be taken. I will also let the participants know that no identifying information such as name, address, and the organization name will be used. I will tell them that all interview material will be encrypted and stored in a locked container accessible only by the researcher. 5 Proceed with the interview once the participant indicates readiness to begin and start audio recording.
Interview Questions	<ol style="list-style-type: none"> 1 What strategies do you use to secure your organizations network(s) from cyberattacks? 2 How do you conduct risk assessments in your organization, and how do you decide which threats to address first? 3 What factors do you consider most critical when identifying cyberattack risks in your network security strategies? 4 How do you integrate external threat intelligence into your risk management practices to anticipate and prevent cyberattacks? 5 Can you describe a time when you had to adjust your risk management strategy in response to an evolving cyber threat? 6 How does your organization adapt to emerging threats? 7 What types of internal controls have you implemented to secure your organization's network, and how do you evaluate their effectiveness? 8 How do you ensure that internal controls such as access control, encryption, and multi-factor authentication are appropriately applied? 9 How do you address training staff to follow security protocols or prevent mistakes? 10 Can you share an example of a security incident where your internal controls helped secure your organization's network from a cyberattack?
Conclusion	<p>Inform the participants that a follow-up interview will be conducted to review my interpretation of their answers and schedule the interview. Stop audio recordings and thank the participant for participating in the study.</p>
