

European International University, EIU-Paris

Doctoral Thesis

Research in Cybersecurity Risk in Emerging Technology

Submitted by:

SUSHANTH NAIR

[EIU925107]

In Partial fulfillment of the Requirements for the Degree of

Doctor of Engineering in Computer science

Supervisor:

Prof. (Dr.) S. Edmund Christopher

Date:

December, 2024

DECLARATION

I hereby declare that the work in this thesis entitled, “Research in Cybersecurity Risk in Emerging Technology” has been undertaken and completed by me for the award of the degree of **Doctor of Engineering in Computer science** with European International University, under the guidance of Prof. (Dr.)S. Edmund Christopher.

I also declare that this thesis is an original work and has not been submitted for any degree or diploma in any other university or institution. Further, I declare that the texts, figures, tables, and any other material taken from other sources has been acknowledge, referred and cited in the best of my knowledge and understanding



Signature of Research Scholar,

Sushanth Nair

European International University

Date: December 2024

Place: Singapore

CERTIFICATE OF ORIGINALITY

This is to certify that the thesis entitled “Research in Cybersecurity Risk in Emerging Technology” is a Bonafide research work conducted by SUSHANTH NAIR

in partial fulfilment of the requirements for the award of the **Doctor of Engineering in Computer science** degree from the European International University (EIU-Paris). This research was carried out under my supervision and guidance.

The thesis represents an original work undertaken in accordance with the academic regulation of the European International University. This content of this thesis reflects the independent research efforts of the candidate. This thesis has not been submitted for the award of any degree, diploma, or other qualification at any other university



Signature of Supervisor

Prof. (Dr.) S. Edmund Christopher

Date: December 2024

Place: UAE

UNIVERSITY APPROVAL

This dissertation titled, “Research in Cybersecurity Risk in Emerging Technology” has been examined and approved by the European International University (EIU-Paris) for the award of the **Doctor of Engineering in Computer science.**

Signature:



Name: Ky. Col. Prof. Dr. Edward Roy Krishnan

Position: Founder & Director General

European International University, Paris, France

Date: January 15th, 2025

University Seal:

Abstract

Introduction - The current study examines the changing cybersecurity threats brought about by the incorporation of cutting-edge technologies. These technologies have drastically changed risk topologies and made vital infrastructure vulnerable to advanced cyberthreats, even if they also foster innovation and operational efficiency. The study points out a significant vacuum in the literature by pointing out that although there are generic cybersecurity frameworks, they do not adequately contextualize the dangers posed by autonomous, decentralized, and linked systems. The study lays forth goals to pinpoint the main weaknesses, assess risk management, and provide customized mitigation strategies for these technologies.

Literature Review - The review highlights that cybersecurity in the digital age encompasses a dynamic, adaptive infrastructure with AI-powered intelligence, accurate device interaction, and distributed data management, rather than only protecting static networks. It distinguishes between risk, vulnerability, and danger and describes how new technologies provide new vectors, including smart contract attacks, quantum decryption, and adversarial AI manipulation. The literature also criticizes current models, like as NIST RMF and ISO 27001, for their poor suitability for autonomous systems, decentralized platforms, and edge computing. Cross-disciplinary perspectives such as strategic resilience, legal fragmentation, and ethical governance are included in the literature.

Methodology - Using a standardized Likert-scale questionnaire, the study takes a quantitative approach and targets industry experts and cybersecurity specialists. Purposive sampling ensured that respondents had relevant expertise with the deployment of developing technologies. Statistical methods were used to evaluate the data and investigate the connections among readiness levels, technology-specific weaknesses, and perceived risk. Respondent confidentiality, informed consent, and data privacy were all strictly adhered to as ethical principles.

Results & Findings - According to the findings, 76% of respondents pointed out that IoT devices lacked sufficient firmware and encryption safeguards, while 89% of respondents said AI systems were susceptible to adversarial assaults and data poisoning. The main hazards associated with blockchain technology are vulnerabilities in smart contract logic and theft of private keys. Quantum computing was seen as an existential danger to existing encryption

standards, and cloud settings continued to be vulnerable to misconfiguration and uncertainty over shared responsibility. Compounding problems included fragmented governance, a shortage of qualified personnel, and regulatory unpreparedness.

Discussion & Conclusion - The discussion highlights how system interdependencies and inadequately integrated security models caused by new technologies increase risk. According to the study's findings, traditional cybersecurity models are no longer relevant in light of emerging technologies. It suggests a multi-layered, context-aware risk governance framework that prioritizes proactive incident readiness, ethical safeguards, adaptive strategies, and cross-border regulatory cooperation. It urges continued investigation of multidisciplinary, scalable security frameworks that are in line with quickly changing digital environments.

Table of Contents

Abstract 5

1. Chapter 01 – INTRODUCTION 13

1.1 Background of the Study 13

1.2 Problem Statement 15

1.3 Purpose of the Research 18

1.4 Research Objectives 19

1.5 Research Questions 19

1.6 Research Gap 20

1.7 Scope of the Study 21

1.8 Significance of the Study 22

1.9 Organization of the Dissertation 24

2. Chapter 02 – LITERATURE REVIEW & CONCEPTUAL FRAMEWORK 25

2.1 Key Concepts 25

2.1.1 Cybersecurity 25

2.1.2 Emerging Technologies 30

2.2 Overview of Cybersecurity 36

2.2.1 Evolution of Cybersecurity 36

2.2.2 Core Concepts 37

2.2.3 Cybersecurity Challenges in the Digital Age 39

2.3 Overview of Emerging Technologies 40

2.3.1 Artificial Intelligence & Machine Learning 40

2.3.2 Internet of Things 42

2.3.3 Blockchain Technology 43
2.3.4 Cloud Computing 44
2.3.5 Quantum Computing 45
2.3.6 Integration of Emerging Technology 46
2.4 Current State of Cybersecurity in Emerging Technologies 46
2.5 Cybersecurity Risks in Emerging Technologies 49
2.5.1 Threat Landscape 49
2.5.2 Vulnerabilities in Emerging Technologies 52
2.6 Challenges in Managing Risks in Emerging Technologies 54
2.6.1 Organizational Challenges 55
2.6.2 Technical Challenges 56
2.6.3 Regulatory Challenges 58
2.7 Theoretical Framework 59
2.7.1 The Risk Management Framework 60
2.7.2 Technology Acceptance Model 62
2.7.3 Diffusion of Innovation Theory 64
2.8 Research Hypothesis 67
3. Chapter 03 – RESEARCH METHODOLOGY 69
3.1 Research Philosophy 69
3.1.1 Pragmatism Philosophy 69
3.1.2 Positivism Philosophy 69
3.1.3 Interpretivism Philosophy 70
3.1.4 Realism Philosophy 70

3.2 Research Approach 70
3.2.1 Inductive Approach 71
3.2.2 Deductive Approach 71
3.2.3 Abductive Approach 71
3.3 Research Strategy 72
3.3.1 Quantitative Strategy 72
3.3.2 Qualitative Strategy 73
3.3.3 Mixed-Method Strategy 73
3.4 Data Collection Procedure 73
3.4.1 Primary Source of Data Collection 74
3.4.2 Secondary Source of Data Collection 74
3.5 Data Collection Tools 75
3.5.1 Observation 75
3.5.2 Interviews 75
3.5.3 Survey 75
3.6 Population & Sample Size 76
3.7 Sampling Technique 77
3.7.1 Probability Sampling 77
3.7.2 Non-Probability Sampling 78
3.8 Description of Participants of the Study 78
3.9 Research Tool & Development 79
3.10 Data Analysis 80
3.10.1 Thematic Analysis 81

3.10.2 Content Analysis 81
3.10.3 Statistical Analysis 81
3.10.4 Narrative Analysis 81
3.11 Ethical Considerations 82
3.11.1 Informed Consent 83
3.11.2 Anonymity & Confidentiality 83
3.11.3 Updating Participants 83
3.11.4 Respect-Based Ethics 84
4. Chapter 04 – RESULTS & FINDINGS 85
4.1 Respondent Demographics 85
4.1.1 Age 85
4.1.2 Gender 86
4.1.3 Highest Educational Qualification 87
4.1.4 Current Role / Job Title 88
4.1.5 Years of Experience in IT / Cybersecurity 90
4.1.6 Company's Primary Technology Focus 91
4.2 Descriptive Statistics 93
4.3 Results 100
4.4 Summary of Hypothesis 118
5. Chapter 05 – DISCUSSION & RECOMMENDATION 120
5.1 Discussion of Results & Findings 120
5.2 Conclusion 124
5.3 Implications of the Study 125

5.3.1 Theoretical Implications 125
5.3.2 Managerial Implications 126
5.4 Limitations of the Study 127
5.5 Recommendations 129
5.5.1 For Improvements 129
5.5.2 For Future Research 130
6. References 132
7. Appendix 153
7.1 Questionnaire 153
7.1.1 Section A - Demographic Information 153
7.1.2 Section B – Research Questions 154

List of Tables

Table 1: Definition of Cybersecurity by Different Authors 26

Table 2: Definition of Emerging Technologies by Different Authors 31

Table 3: Technical Challenges in Emerging Technologies for Cybersecurity Risks 57

Table 4: Age Distribution of Participants 85

Table 5: Gender Distribution of Participants 86

Table 6: Highest Educational Qualification of Participants 87

Table 7: Current Role / Job Title of Participants 88

Table 8: Respondents' Years of Experience in IT / Cybersecurity 90

Table 9: Respondents' Firm's Primary Technology Focus 91

List of Figures

Figure 1: Risk Management Framework (RMF) 60

Figure 2: Technology Acceptance Model (TAM) 62

Figure 3: Characteristics of Diffusion Innovation Theory 64

Figure 4: Adopter of DOI Theory 66

1. CHAPTER 01 – INTRODUCTION

1.1 Background of the Study

In today's quickly changing digital landscape, new technologies like cloud computing, blockchain, machine learning (ML), autonomous cars, artificial intelligence (AI), and the Internet of Things (IoT) are transforming many industries, including manufacturing, healthcare, finance, and education (Lewallen, 2021). While technology presents an opportunity for efficiency and innovation, organizations also need to address emerging cybersecurity concerns. By incorporating these technologies into already-existing infrastructures, the attack surface is increased and new vulnerabilities are introduced that might not be sufficiently addressed by conventional cybersecurity methods (Umoga et al.,2024). For example, the decentralized structure of blockchain technology presents issues for data integrity and system compatibility even as it provides improved security in certain ways. Likewise, the IoT poses risks to unauthorized access, data privacy, and the exploitation of private information attributable to its many connected gadgets (Jimmy, 2021). Furthermore, a key component of the cybersecurity equation is still the human factor. Even with the huge technological improvements, security breaches frequently continue to happen. Human error, which is stereotypically caused by insufficient training or ignorance, is the main cause of this. Besides, because laws are incapable of keeping ahead of technological shifts, corporations encounter difficulties with compliance (Thach et al., 2021). The use of technologies augments the intricacy of cybersecurity, requiring an inclusive strategy that takes into consideration human, organizational, and legal issues in addition to technical ones.

In history, cybersecurity strategies had been established in the framework of traditional information systems, in which networks had comparatively distinct boundaries and data was saved on centralized servers (Wynn, & Bechkoum, 2024). However, as emerging technologies have developed, these lines have turn out to be less distinct, and the attack shallow has grown. For instance, IoT devices frequently lack encryption and authentication systems, making them prime targets for cyber attackers (Saeed et al., 2023). These devices are characterized by limited computing power and weak security protocols. As demonstrated in the 2016 Mirai botnet event, which affected major websites by taking advantage of unprotected IoT devices (Almazarqi, 2024), compromised IoT devices can be used as entry points for more extensive network

incursions or as weapons in distributed denial-of-service (DDoS) operations. Likewise, AI possesses dual-use properties, meaning that the same technologies that are employed to improve cybersecurity, like threat prediction and anomaly detection, can also be utilized by hostile actors to launch clever and flexible attacks (Tusher et al., 2022). For instance, malicious machine learning compromises the credibility of security applications such as intrusion detection systems, spam filters, and facial recognition by tampering with input data to trick AI systems (Mızrak, 2023). In addition, the fact that many AI algorithms are black-boxes makes threat mitigation more challenging because their decision-making procedures are frequently opaque and challenging to audit.

Although blockchain technology is praised for its decentralized trust model and immutability, it also poses a unique set of cybersecurity issues. Blockchains are not impervious to attacks, despite their intrinsic protection against some forms of data manipulation (Okafor et al., 2023). It has been discovered that smart contracts, a fundamental component of many different blockchain platforms, have weaknesses in logic and re-entrancy. A badly written smart contract was the main cause of the infamous Decentralized Autonomous Organization (DAO) attack in 2016, which saw the theft of over 50 million US dollars' worth of cryptocurrencies (Scharfman, 2024). Meanwhile, private keys that are utilized for logging into blockchain assets continue to be an important single point of failure because they are more difficult to modify or cancel once hacked than traditional credentials (Mahmood et al., 2022). Real-time interactions between millions of devices are made possible by the introduction of 5G networks, which offer low-latency communication and high-speed connectivity. Nevertheless, 5G architectures distributed and software-defined characteristics make them more complicated and provide opportunities for cyberattacks. From software errors in virtualized network functions (VNFs) to unsafe hardware components, major vulnerabilities in the 5G supply chain have been found. These vulnerabilities can be used by threat actors to carry out advanced persistent threats (APTs) (Lyu et al., 2024), espionage, or interfere with critical services.

Even though it is currently in its early stages of development, quantum computing could eventually jeopardize cybersecurity because it could crack popular cryptographic techniques (Baseri et al., 2024). By factoring huge integers exponentially quicker than classical algorithms, quantum techniques like Shor's algorithm threaten the security of elliptic curve and RSA

cryptography. International attempts to study post-quantum cryptography have already been driven by the predicted threat of quantum decryption (Csenkey & Bindel, 2023). When quantum capabilities advance, current encrypted data may become retrospectively susceptible since many infrastructures are still unprepared for a quantum-enabled adversary. These illustrations highlight how urgently cybersecurity strategies must be adjusted to take into account the distinctive characteristics and attack vectors developed through emerging technology (Nookala et al., 2024). The main reason why current security frameworks frequently fail to meet these changing issues is that they are generic instead of context-specific and reactive rather than proactive. Given the context of emerging technology, cybersecurity necessitates not only technological controls but also strong risk assessment models, regulatory and legal frameworks (Oyewole et al., 2024), continual research to predict and prevent new threats, and cross-sector collaboration.

Cybersecurity risk management is further complicated by the geopolitical environment. The use of cyber capabilities by nation-states for sabotage, cyberespionage, and power projection is growing (Möller, 2023). Strategic vulnerabilities are created when emerging technologies are incorporated into vital national infrastructure, such as defence systems, banking networks, and power grids. If these vulnerabilities are taken advantage of, they could cause significant disruption and loss. A state-sponsored actor was implicated in the 2020 SolarWinds supply chain hack, which demonstrated how skilled attackers may compromise reliable software components to concurrently enter numerous government and commercial sector networks (Cordey, 2023). The risk is increased by the absence of uniform cybersecurity regulations and compliance procedures among countries. For example, the adoption of new technology frequently outperforms the development of strong cybersecurity laws and institutional capability in many developing nations (Branley-Bell et al., 2022). These areas are especially susceptible to cybercrime because of the digital divide. The development of a coherent cybersecurity defence posture is complicated even in technologically sophisticated countries by regulatory delays and disjointed monitoring (Ahmed et al., 2022), such as disparate data protection legislation and inconsistent business practices.

1.2 Problem Statement

The current digital ecosystem has undergone a substantial transformation due to the rapid growth of emerging technologies like blockchain, quantum computing, AI, IoT, and 5G networks

(Beshley et al., 2021). These technologies offer previously unheard-of opportunities for innovation, efficiency, and connectivity in different industries, such as finance, transportation, healthcare, and defence (Cains et al., 2022). However, they also carry with them new and intricate cybersecurity risks that are not well understood, not sufficiently regulated, and not well moderated within the cybersecurity frameworks that are presently in place. This gap between technology development and cybersecurity preparedness is a serious and unique research problem that demands instant academic and policy-level action.

The problem is not only that emerging technologies exist; it's also that the cybersecurity risks that they cause have evolved in both their nature and topology. With these new digital paradigms, traditional cybersecurity methods that were built on traditional IT systems are becoming less and less effective in anticipating, identifying, and mitigating risks (Kalinin et al., 2021). Blockchain's decentralized architecture, for example, has created new avenues for exploitation, like Sybil attacks and smart contract vulnerabilities, despite being intrinsically safe in some ways (Dwivedi et al., 2024). According to the exponential increase in botnet-driven DDoS attacks, IoT devices are one of the most abused attack surfaces nowadays due to their low processing capacity and lack of defined security measures. The incorporation of AI into cybersecurity technologies has two disadvantages: although it can improve threat detection skills, it also gives attackers the ability to launch clever, adaptive, and autonomous cyberattacks (Sarker, 2024).

The absence of organized risk assessment models that are adapted to the unique features associated with every emerging technology is one of the most challenging aspects. It is frequently difficult for traditional risk assessment techniques, like ISO 27005 or the NIST Risk Management Framework, to capture the ever-changing and unpredictable nature of hazards related to technologies like artificial intelligence or quantum computing (Barlybayev et al., 2024). For example, popular cryptography using public key systems like RSA and ECC is at existential risk from quantum computing. However, there are currently no defined implementation frameworks for mitigation measures, and most mitigation strategies are theoretical or in the early stages of development (Radanliev, 2023). The disparity between theoretical knowledge and real-world security preparedness reveals how unique and pressing the problem is.

Furthermore, risk governance is made more difficult by the transdisciplinary character of developing technologies. In technologies such as brain-computer interfaces (BCIs) or biomedical IoT devices, the intersection of computing, biology, engineering, and cognitive sciences demands a multifaceted cybersecurity strategy that goes beyond traditional IT controls (Piszcz et al., 2024). The majority of cybersecurity regulations, however, are still compartmentalized inside industry-specific borders and lack the ability to integrate threats from the digital, biological, and physical realms (Chiara, 2022). The situation is made worse by the lack of a unified regulatory and compliance framework, which forces many stakeholders, including governments, commercial companies, developers, and end users, to function with disjointed or antiquated security requirements.

The gap between workforce development and cybersecurity education and the rate of technology advancement is another important factor. Businesses that use emerging technologies frequently lack the cybersecurity expertise necessary to identify or reduce the dangers specific to these platforms. SMEs without specialized cybersecurity teams are especially affected by this skill gap, which results in incorrect configurations, slow incident responses, and inefficient remediation techniques. This increases the vulnerability of the entire ecosystem by making these organizations obvious targets for cybercriminals.

The problem's specificity and severity are supported by empirical data. A 2024 World Economic Forum research claims that cyberattacks on platforms for developing technologies have increased by over 40 percent yearly, putting key infrastructure at ever-greater risk (Kudzko, & Burilkov, 2025). The 2021 Colonial Pipeline ransomware attack serves as an example of the domino effect of cybersecurity lapses in technologically enhanced surroundings (Temitope Olayinka, 2025). The attack took advantage of IoT and remote access weaknesses. There are still few technology-specific, context-specific risk models across both academic research and business practice, despite these cautions. In cybersecurity management, operational decision-making and strategic planning are impeded by the absence of quantitative risk indicators specific to developing technologies (Mızrak, 2023).

Cybersecurity regulations are subject to jurisdictional uncertainties and inconsistencies due to the global nature of developing technology deployment (Qian, 2024). Cyber attackers can take advantage of gaps created by asymmetric enforcement capabilities, disparate legal standards, and

cross-border data flows. Since blockchain and artificial intelligence frequently function in decentralized or international contexts, this legal fragmentation is especially problematic for these technologies. Risk mitigation initiatives are likely to remain ineffectual and inconsistently executed in the absence of standardized cybersecurity standards and international cooperation channels (Qudus, 2025).

To make problems worse, nothing has been identified about the ethical ramifications of cybersecurity for emerging technology. Apart from technological vulnerabilities, there are also socio-ethical issues associated with AI systems educated on inaccurate information, autonomous drones deployed for surveillance, and digital twins used in healthcare systems (Filipenko et al. 2024). These include algorithmic discrimination, privacy violations, and the decline in confidence in digital systems. There are currently insufficient thorough studies that incorporate ethical risk within cybersecurity models for developing technologies, which further limits the development of complete security frameworks.

In light of these challenges, the main issue this study attempts to address is the inadequate modelling, conceptualization, and governance of cybersecurity threats in the context of emerging technologies. This issue is not just theoretical or speculative; it shows up as actual risks that exist, quantifiable losses, and strategic blind spots that jeopardize national security, economic stability, and technological advancement. This research aims to fill a main research gap that is selected by the lack of tailored cybersecurity risk frameworks, the incompetence of current guidelines, the lack of competent employees, and ethical blind spots.

1.3 Purpose of the Research

The purpose of this study is to perform research into the extent, categories, and management of cybersecurity risks associated with the utilization and application of emerging technologies, with special concentration on AI, blockchain technology, the IoT, cloud computing and quantum computing. Although these technologies have the potential to be innovative, they also present new attack sides and vulnerabilities that traditional cybersecurity frameworks are ill-prepared to manage. The research intends to examine how these risks transform in dynamic technology ecosystems and evaluate how well-matched the existing risk assessment models are for forestalling and decreasing risks in these settings.

1.4 Research Objectives

The research purpose is to explore and analyze the strategies employed to manage cybersecurity risks in developing technologies. With regard to developing technologies, the study explicitly intends to:

- To identify and classify the major cybersecurity risks associated with emerging technologies.
- To evaluate the vulnerabilities inherent in these technologies that contribute to heightening cyber risk.
- To analyze existing cybersecurity frameworks and their efficiency in mitigating risks within emerging technologies.
- To investigate targeted cyberattacks on emerging technologies and assess their operational and technical impacts.
- To explore the organizational, technical, and regulatory challenges involved in managing cybersecurity risks in emerging technologies.
- To assess the preparedness of governments and industries in addressing cybersecurity challenges posed by emerging technologies.

1.5 Research Questions

In association with the above research objectives, some research questions were developed, which are given below:

- What are the major cybersecurity risks associated with emerging technologies?
- What inherent vulnerabilities in these technologies contribute to heightening cyber risk?
- How efficient are existing cybersecurity frameworks in mitigating risks within emerging technologies?
- What are the operational and technical impacts of targeted cyberattacks on emerging technologies?

- What organizational, technical, and regulatory challenges do stakeholders encounter in managing cybersecurity risks in emerging technologies?
- How prepared of governments and industries in addressing cybersecurity challenges posed by emerging technologies?

1.6 Research Gap

The technical landscape is changing across industries due to emerging technologies. However, little has been researched about how these developments may affect cybersecurity in both academic and real-world settings. Although the body of research on generic cybersecurity principles is expanding, there is still a significant study deficit in the areas of risk detection, categorization, and management that are specific to these technologies. Studies that have already been done are generally disjointed and concentrate on discrete technologies without acknowledging how they overlap or the increased security threats that result from their integration.

Additionally, established cybersecurity frameworks such as NIST and ISO 27001 were created for traditional IT settings and have little relevance for autonomous, decentralized, and real-time systems. There is not enough empirical data to assess how well these frameworks operate with new technology, especially in high-risk industries like critical infrastructure, healthcare, and finance. Furthermore, organizational, legal, and regulatory issues that impede efficient cybersecurity governance in quickly changing digital ecosystems receive little attention in the majority of current research, which focuses primarily on technical vulnerabilities.

Another significant gap is the absence of sector-specific and national comparative evaluations, particularly with regard to the preparedness of industries and governments in nations with low or middle incomes. This includes limitations in incident response capacity, cybersecurity talent development, and threat intelligence. A multidisciplinary strategy combining technological, strategic, and policy aspects is needed to close these gaps. By providing a thorough assessment of cybersecurity risks and responses adapted to the intricacies of developing technologies, this study seeks to close this gap.

1.7 Scope of the Study

The identification, categorization, and evaluation of cybersecurity risks related to particular emerging technologies are the particular subject matter of this research, with a focus on the technical, operational, organizational, and regulatory aspects of these risks. Artificial intelligence, the Internet of Things, blockchain technology, 5G communication networks, and quantum computing are among the cutting-edge technologies that are being investigated in this study. These technologies were chosen because of their widespread use in vital industries like healthcare, manufacturing, energy, finance, and defence, as well as because of their known or predicted vulnerability to cybersecurity risks that put conventional security approaches to the test (George et al., 2024).

Both industrialized and developing countries are included in the study's geographic coverage, with an emphasis on comparing cybersecurity readiness across various technical and legislative contexts. Although the study has a global scope, it focuses on particular instances from nations and areas that have shown a significant interest in implementing emerging technology, including the US, the EU, China, India, and a few Middle Eastern and African countries (Lameijer et al., 2021). In order to properly understand the disparities in preparedness, policy creation, and infrastructure maturity in tackling cybersecurity risks, a comparative approach is required.

The study's approach allows it to examine cybersecurity risks at three interrelated levels: incident-level impacts, organizational and regulatory responses, and technological vulnerabilities. At the technological level, this research investigates how distinct risk vectors are produced by the system topologies, dependence on data, and communication protocols that are inherent in each evolving technology. For example, the study delves into network slicing risks in 5G, adversarial assaults in AI systems, unsecured communication in IoT ecosystems, blockchain smart contract issues, and quantum decryption threats (Alanazi, 2023). At the incident impact level, the study examines and evaluates recorded cyberattacks or security breaches employing new technology, looking at the effects on operations, finances, and reputation. The integration of case studies and threat intelligence reports illustrates real-world situations and identifies typical risk trends. These instances are examined critically in order to show both the limitations of the defences in place, along with the structural vulnerabilities that enemies take advantage of (Steingartner et al., 2021).

The regulatory and organizational level of study evaluates how ready governments and industries are to put in place efficient cybersecurity measures. This involves assessing the strength of legal frameworks governing the safe implementation of emerging technologies, human resource capacities, incident response procedures, cross-sector cooperation, and security frameworks (such as NIST, ISO 27001, and national cybersecurity initiatives) (Brezavšček, & Baggia, 2025). The research primarily looks at how ineffective cybersecurity risk management is disadvantaged by fragmented governance, uneven policy enforcement, and technological illiteracy. Essentially, this research does not concentrate on general cybersecurity procedures or legacy IT systems outside of the framework of developing technology. Additionally, it is attempting to close the knowledge gap within strategic risk awareness and governance frameworks rather than trying to create innovative security algorithms or offer comprehensive technical solutions. In the quickly changing field of emerging technologies, this research is positioned to offer practical insights for academic researchers, technology developers, cybersecurity experts, and governments working to improve resilience against cyber threats.

1.8 Significance of the Study

The significance of this research depends on its ability to contribute to knowledge, assessment, and strategic management for cybersecurity risks, particularly those related to emerging technologies. The implementation of emerging technologies has recently become essential to the operations and infrastructure of vital industries like healthcare, finance, transportation, energy, and defense as the world's digital transformation builds rapidly (Attah et al., 2024). However, existing frameworks are insufficiently prepared to handle the numerous and frequently unexpected cybersecurity risks that are generated by these technologies. Therefore, this research is crucial to addressing important knowledge gaps at the interface of cybersecurity risk management and technological innovation.

From a theoretical standpoint, the study adds a multifaceted framework for assessing hazards in developing technologies, which advances the scholarly conversation on cybersecurity. The research offers comprehensive, technology-specific observations that can guide future scholarly work on cybersecurity, as opposed to viewing it as a generalized or static issue. It also adds to the existing body of knowledge by combining organizational behavior, policy analysis, and technical threat models. This emphasizes how systemic weaknesses result from insufficient

institutional, legal, and operational procedures in addition to technological vulnerabilities (Liu, & Lu, 2021).

For organizations and industries, the current research provides recommendations on how to meet cybersecurity expenses to particular risk profiles related to emerging technology. Many businesses are prioritizing speed and utility over security as they implement digital transformation plans (Saeed et al., 2023). The long-term expenses and operational interruptions brought on by insufficient security measures are highlighted in this study, which also promotes comprehensive cybersecurity planning that crosses the technical, governance, and human layers. Additionally, it highlights important organizational issues that need to be resolved in order to improve cybersecurity resilience, such as a lack of skilled personnel, disjointed governance, and inadequate incident response preparedness.

For professionals and practitioners in cybersecurity, the study provides a research-based comprehension of new technology-specific risk drivers. Through an analysis of actual cyber incidents, system weaknesses, and the effectiveness of current security measures, the research offers practical insights that can guide the development of flexible cybersecurity plans (Goni et al., 2024). For instance, experts can proactively improve their risk identification and response skills by comprehending how criminal machine learning weakens AI systems or the manner in which zero-day vulnerabilities within 5G network slicing are capable of being exploited (Fakhouri et al., 2023). The study also identifies vulnerabilities in existing frameworks and standards, assisting practitioners in creating stronger, context-specific procedures.

For regulators and policymakers, the study is important as well since it highlights how inadequate the current regulatory and legal frameworks are at handling cybersecurity risks driven by quickly changing technologies. Regulatory tools frequently fall behind technical advancements in many jurisdictions, creating legal ambiguities and difficulties with enforcement (Fakhouri et al., 2023). This analysis emphasizes how urgently coordinated, forward-thinking, flexible, and technologically aware cybersecurity governance rules are needed. The significance of cross-border regulatory collaboration is emphasized, especially when it relates to tackling transnational risks while developing standards for technologies such as blockchain and quantum computing.

For decision-makers and industry leaders, the study highlights the strategic significance of cybersecurity in technical investments and innovation strategy. Understanding the cybersecurity risk landscape is essential to preserving operational resilience, compliance with laws and regulations, and customer trust as businesses use AI, IoT, and blockchain-based systems more frequently. According to Kosutic, & Pigni, (2022), companies should invest enough money in developing organizational cybersecurity capabilities and incorporate cybersecurity into the early phases of technology adoption.

1.9 Organization of the Dissertation

There are five separate chapters to the research.

Chapter 01: The Introduction chapter provides the background of the study, statement of the problem, research objectives, and research questions, along with the research gap, scope, significance of the study, scope of the study, and organization of the study.

Chapter 02: The Literature Review chapter involved key concepts, overview of cybersecurity, overview of emerging technologies, current state of cybersecurity in emerging technologies, cybersecurity risks in emerging technologies, challenges in managing risks in emerging technologies, theoretical framework, and research hypothesis.

Chapter 03: The Research Methodology chapter involved the research philosophy, research strategy, research approach, data collection tools, data collection procedure, sampling technique, population and sample size, participant description, data analysis, research tool and development, and ethical considerations.

Chapter 04: The Results & Findings chapter is devoted to the analysis and presentation of the results, which include the demographics of the respondents, descriptive data, and a summary of the hypothesis.

Chapter 05: The Discussion & Recommendations chapter discusses and presents the study's implications, limits, and results and findings as well as its conclusions, recommendations for improvement, and recommendations for further research.

2. CHAPTER 02 – LITERATURE REVIEW & CONCEPTUAL FRAMEWORK

2.1 Key Concepts

2.1.1 Cybersecurity

The word "cybersecurity" has been used in academic and popular literature, much of which has taken a certain stance on the issue. The term is used widely, and its definitions are very diverse, context-bound, subjective, and occasionally uninformative, according to the literature review. Little research has been undertaken on the term's actual meaning and how it is used in different circumstances. In the absence of a succinct, widely accepted definition that encompasses the multifaceted nature of cybersecurity, technological and scientific advancements may be hampered by the reinforcement of the primarily technical perspective of cybersecurity and the division of disciplines that should collaborate in order to address complex cybersecurity issues.

According to Lewallen, (2021), the area of cybersecurity is surrounded by a number of interconnected discourses. By dissecting the term "cybersecurity," some of the legacy problems are exposed, and the conversation is placed inside the contexts of "cyber" and "security." The prefix "cyber" denotes cyberspace and is used to describe virtual reality and electronic communication networks (Cains et al., 2022). According to Schiliro (2023), it developed from the term "cybernetics," which denoted the "domain of communication and control theory, either in animal or in machine". By describing his vision of a three-dimensional environment of pure information that moves between computers and computer clusters where individuals are both information creators and users, William Gibson popularized the word "cyberspace" in his 1984 novel Neuromancer (Taherdoost, 2022).

On the other hand, according to the literature we reviewed, the term "security" has a notoriously difficult definition in the general sense, and there doesn't seem to be a widely acknowledged idea (Latino, & Menegoli, 2022). Maurer, & Morgus, (2022) assert that security discourses must inevitably cover and aim to comprehend who securitizes, on what issues (threats), for whom (the referent object), why, with what outcomes, and under what circumstances (the structure). The concept of security can take on different meanings depending on one's viewpoint and values, even while there are more tangible forms of security (such as the physical, human, or information system qualities or mathematical definitions for different types of security).

Table 1: Definition of Cybersecurity by Different Authors

Author	Element	Definition
Von Solms & Van Niekerk (2013)	Conceptual Foundation	Cybersecurity implies the thorough protection of data assets using a socio-technical approach that goes beyond conventional technical controls and includes governance, guidelines, awareness, and culture. It also includes risk management for the whole cyber ecosystem.
Craigen et al., (2014)	Multidimensional Scope	Cybersecurity is an interdisciplinary field that includes law, policy, technology, and human behavior. It seeks to protect and maintain the CIA (confidentiality, integrity, and availability) of cyberspace, encompassing networks, devices, systems, and data in both the public and commercial sectors.
Singer & Friedman (2014)	National Security Dimension	Cybersecurity is a vital national security issue, as the digital realm turns into a battlefield for geopolitical domination, espionage, and cyberwarfare. The protection of a country's intellectual property and vital infrastructure from cyberattacks by non-state actors, as well as state actors, is included.
Bada et al., (2019)	Behavioral Perspective	Cybersecurity is not just a technical problem; human actions, attitudes, and judgments play a significant role. To lessen vulnerabilities brought on by bad cyber hygiene and social engineering threats, ongoing user involvement, security instruction, and behavioral interventions are

		needed.
Pfleeger & Pfleeger (2012)	System Security	Cybersecurity refers to the use of technologies and methods that enforce acceptable behavior norms in digital systems. To guarantee secure and validated system interactions, these consist of intrusion detection, cryptography, authentication, access control, and monitoring.
Kostopoulos (2013)	Risk-based Approach	Cybersecurity is an organized method for detecting, evaluating, reducing, and keeping an eye on cyberthreats related to operational flaws, external threats, and system vulnerabilities, especially those that target valuable assets and vital infrastructure.
International Telecommunication Union (ITU, 2008)	Global Policy Framework	Cybersecurity is a collection of best practices, policies, procedures, and technology that are intended to safeguard users' and organizations' assets as well as the cyber environment. At the national and international levels, it includes administrative, technical, and legal measures.
European Union Agency for Cybersecurity (ENISA, 2016)	Operational Resilience	The ability to defend digital infrastructure against online assaults and recover from them is known as cybersecurity. Throughout the EU and beyond, it emphasizes threat intelligence sharing, incident response collaboration, and resilience to reduce risks and maintain digital trust.
Sharma & Chen (2020)	Emerging Technology Focus	In the context of artificial intelligence, the Internet of Things, blockchain, and 5G, cybersecurity refers to the management of vulnerabilities present in decentralized, highly

		intelligent, and autonomous systems. Context-specific safeguards like adaptive access control, dynamic authentication, and moral AI governance are necessary for this.
Gonzalez-Granadillo et al. (2020)	Automation in Cybersecurity	In order to provide real-time protection in intricate digital settings, cybersecurity involves automating risk identification, response, and mitigation procedures. The objective is to provide ongoing security monitoring and reduce human latency in crucial processes.
Bayuk et al. (2012)	Governance Integration	Cybersecurity is the application of enterprise-wide governance procedures and policies that are intended to match business goals with IT security. It incorporates audit, control, compliance, and risk management into fundamental organizational procedures.
Tipton & Krause (2007)	Infrastructure Protection	The purpose of cybersecurity is to protect the many levels of infrastructure, from hardware to applications, against intrusions, attacks, and interruptions. It prioritizes proactive risk management and backup plans while utilizing tiered defence mechanisms.
Safa et al., (2016)	User Awareness & Culture	An essential component of cybersecurity is end-user awareness. Even the strongest technical safeguards can be compromised by carelessness, social engineering, or deliberate wrongdoing if an organization's culture is not security-focused.
National Institute of Standards and	Standardized	The defense of information systems against unwanted access, utilization, disclosure,

Technology (NIST, 2018)	Framework	interruption, alteration, or destruction is known as cybersecurity. Five fundamental functions, identification, protection, detection, response, and recovery, guide this ongoing risk-based process, according to NIST.
Huang et al. (2011)	Cybersecurity Metrics	In order to make proactive and evidence-based decisions, cybersecurity includes the creation of metrics and indicators that allow for a quantitative assessment of the safety record of an organization, risk landscape, and incident response capabilities.
Dhillon & Backhouse (2001)	Ethical & Social Viewpoint	Cybersecurity is more than just safeguarding information and technology; it also involves maintaining moral principles, individual privacy rights, and public confidence in online spaces. Policies and behaviors are fundamentally shaped by ethical issues.
Taddeo (2017)	Cybersecurity Ethics & Trust	Cybersecurity also includes the normative aspects of responsible technology usage, accountability, and digital trust. For cybersecurity to be effective, security measures must be balanced with respect for individual liberty, information freedom, and openness.

In the above table, following the compiled list of academic definitions, cybersecurity is a broad and dynamic field that goes well beyond conventional ideas of technical security. According to Von Solms & Van Niekerk (2013) and Craigen et al. (2014), cybersecurity is fundamentally a socio-technical strategy that combines technology, human behavior, governance, policy, and legislation in order to protect the availability, confidentiality, and integrity of digital systems.

The strategic and national significance of cybersecurity is one important point that many academics have stressed. Singer & Friedman (2014) emphasize the importance of cybersecurity for geopolitical stability and national defence, especially in view of the growing dangers of espionage and cyberwarfare. Similar to this, Sharma & Chen (2020) emphasize how difficult it is to safeguard sophisticated and decentralized systems like blockchain, 5G, IoT, and AI, which require flexible, context-aware defences.

Both the behavioral and human aspects of cybersecurity are equally important. Safa et al. (2016) and Bada et al. (2019) stress that without knowledgeable, watchful users, technical precautions by themselves are insufficient. To reduce human-centric vulnerabilities, behavioral interventions, cultural sensitivity, and education are required. The definitions provided by Bayuk et al. (2012), Rees et al. (2003), and NIST (2018) demonstrate the necessity of integrating cybersecurity into enterprise-wide plans from an organizational and governance standpoint. This involves developing risk-based frameworks, coordinating cybersecurity measures with company goals, and enhancing resilience through standardized procedures. Lastly, researchers such as Taddeo (2017) and Dhillon & Backhouse (2001) broaden the focus to encompass ethical and societal aspects, emphasizing that cybersecurity must safeguard not only data and systems but also core principles like privacy, liberty, and trust.

2.1.2 Emerging Technologies

Emerging technologies are a major topic in policy debates and efforts, and they have generated a lot of disagreement in academic studies. News articles that reference emerging technologies (which is, in their lead paragraphs or headlines) and the expanding number of publications that deal with the topic are signs that the phenomenon of emerging technologies is receiving more attention (Krishnamoorthy et al., 2023). However, growing policy interest in emerging technologies must be weighed against a body of literature that lacks an agreement on what characteristics make a technology emergent. Although the definitions put out by several studies overlap, they also highlight different characteristics.

According to some definitions, for instance, emerging technologies have the potential to have a significant impact on the economy and society (e.g., Porter et al., 2002), particularly when they are more "generic" in nature (Krishnamoorthy et al., 2023). However, other definitions place a greater emphasis on the uncertainty surrounding the emergence process (e.g., Hwang & Chien,

2022) or on the traits of distinctiveness and growth (e.g., Mithas et al., 2022). The viewpoint of the analyst also affects how developing technologies are understood. Because of its uniqueness and anticipated socio-economic significance, a technology may be deemed emergent by some analysts, while others may view it as a logical progression of an already-existing technology. Meanwhile, new technologies are frequently categorized under "general labels" (such as nanotechnology and synthetic biology), but given their distinct socio-technical characteristics (such as technical challenges, involved actors, applications, and uncertainties), they might be best studied independently (Hwang & Chien, 2022).

Table 2: Definition of Emerging Technologies by Different Authors

Author	Element	Definition
Rotolo et al. (2015)	Definition & Criteria	Emerging technologies are distinguished by their radical innovation, comparatively rapid growth, long-term coherence, and potential for large socioeconomic influence. Although they are still in the early stages of development and have not yet gained widespread adoption, their disruptive potential makes them strategically significant.
Cuhls (2010)	Foresight Perspective	Emerging technologies refer to those that are only beginning to be developed and used, but are anticipated to develop over the course of the next five to ten years. Because of the expected revolutionary impact these technologies will have on industry and society, they are being actively monitored using foresight techniques.
Glenn & Gordon (2005)	Innovation Potential	Emerging technologies are described as scientific or engineering advances that have the potential to drastically alter markets, industries, or sectors and establish new paradigms for

		governance, consumption, or production.
Day & Schoemaker (2000)	Strategic Relevance	When accepted early, emerging technologies can give businesses a competitive edge and cause disruptions. Although they still carry a lot of risks and uncertainties, they can change value chains, business models, and customer expectations. They usually start in niches.
Porter et al. (2002)	Technology Lifecycle	Emerging technologies fall within the early stages of the technological lifecycle, which are marked by a great deal of uncertainty, a significant investment in research and development, and an untested potential to make money. These technologies frequently form the basis of prevailing designs in the future.
Dede (2010)	Educational Integration	Emerging technologies in the context of education are digital platforms and tools that provide creative opportunities for instruction and learning. These consist of intelligent tutoring systems, immersive settings (like AR/VR), and adaptable learning platforms, which are not yet widely used.
Linton (2009)	Commercialization Focus	Innovations that are still in the early stages of commercialization or diffusion are referred to as emerging technologies. Their potential for future applications and capacity to reshape markets through novel uses or performance benchmarks are what make them valuable.
Brynjolfsson &	Digital Disruption	With the help of digital intelligence and automated decision-making, the "second

McAfee (2014)		machine age," which is being attributed to emerging technologies like artificial intelligence, machine learning, and robots, continues to redefine labor, economic productivity, and knowledge work.
OECD (2017)	Policy Context	Emerging technologies are those that are still in their infancy but have the potential to have a significant impact on governance, policy, and regulation. Blockchain, artificial intelligence, and neurotechnology are a few examples that pose demands for new legal and ethical frameworks.
Friedman (2006)	Global Connectivity	The global playing field has flattened due to emerging technologies, which reconfigure global corporate dynamics and facilitate distant, distributed collaboration. Examples of these advances include cloud computing, mobile connectivity, and broadband infrastructure.
Brem & Voigt (2009)	Market Disruption	Usually, when emerging technologies enter established markets, they have the ability to seriously upend established players. Industry boundaries are being reshaped by these technologies' alternative value propositions, which may include cost savings, new features, or changes in customer expectations.
Gartner (2023)	Hype Cycle Framework	According to the Gartner Hype Cycle, emerging technologies move from the "Innovation Trigger" towards the "Plateau of Productivity." This model illustrates how the uptake,

		expectations, and visibility of technology change over time. Web3 and generative AI are examples of new technologies.
Nagy et al. (2016)	Social Innovation	Emerging technologies are tools for social transformation in addition to being technological advancements. Their rise is associated with ethical discussions, societal ideals, and new types of user involvement, including in the domains of nanotechnology, genetic editing, and smart monitoring.
U.S. National Science Foundation (NSF, 2018)	Scientific Frontier	It is said that emerging technologies are interdisciplinary breakthroughs that lead to new scientific discoveries. They frequently emerge from fields that are merging, like bioinformatics, nanoscience, and quantum information systems, and necessitate novel experimental techniques and multidisciplinary study.
Bakker et al. (2012)	Uncertainty & Ethical Complexity	There is frequently uncertainty surrounding emerging technologies with regard to their potential uses, hazards, and effects on society. Anticipatory governance is hampered by this ambiguity, particularly in domains like biotechnology, autonomous systems, and AI ethics.
Bozeman et al. (2015)	Public Value Framework	The assessment of emerging technologies should reflect not only on their financial advantages but also their worth to the public, involving whether they improve access,

		sustainability, equity, and transparency in society. These more universal objectives needs to guide the formation of public policy.

The composed definitions of emerging technologies in the above-provided table disclose that emerging technologies are intricate organizations distinguished by their early stages of development, capacity to disrupt various fields (society, science, and the economy), and radical innovation. They are categorized by their high coherence over time, restricted adoption, and ability to pledge long-term structural modification, consistent with authors like Porter et al. (2002) and Rotolo et al. (2015). These technologies are often the outcome of general research and development, and there is a great deal of uncertainty around their social acceptance and commercial viability. Scholars like Day & Schoemaker (2000) and Linton (2009) undermine the benefits of early adoption from a strategic perspective, indicating that emerging technologies have the potential to transform organizational models, restructure value chains, and provide competitive differentiation, although at a significant risk. A beneficial lens for monitoring their growth from early publicity to maturity is presented by tools like the Gartner Hype Cycle (2023).

A policy and ethical viewpoint is vital in addition to economics. Technologies like AI, blockchain, and biotechnology present regulatory and defensive governance challenges, as distinguished by the OECD (2017) and Bakker et al. (2012). This is expanded upon by Bozeman et al. (2015) in their public value framework, which advocates for evaluations that take sustainability, equity, and openness into account. Implications for society and education are equally important. Digital platforms and adaptive learning are the main topics of Dede (2010), but Nagy et al. (2016) present developing technologies as instruments for social innovation that can change user involvement and norms. The NSF (2018) emphasizes its multidisciplinary origins, which stem from the intersection of disciplines such as bioinformatics, nanoscience, and quantum computing.

2.2 Overview of Cybersecurity

2.2.1 Evolution of Cybersecurity

2.2.1.1 Historical Development

The genesis of cybersecurity can be traced back to the advent of the earliest computing systems during the mid-20th century. In the 1960s, as mainframe computers began to be utilized for military and academic purposes, security was largely physical in nature (Singh & Singh, 2024). The need for digital security was minimal, as computing environments were isolated and user access was tightly controlled. The development of the ARPANET (Advanced Research Projects Agency Network) in the late 1960s and early 1970s marked a pivotal moment in cybersecurity history (Packard, 2023). With multiple users and nodes connected over a network, the risk of unauthorized access increased, prompting the first considerations of network security.

One of the earliest formal discussions around computer security was the "Rand Report R-609" in 1970, commissioned by the U.S. Department of Défense (Sipponen, 2022). This report laid the groundwork for what would later become known as the CIA triad: confidentiality, integrity, and availability. It was the first comprehensive document to highlight the necessity of securing information systems against misuse or unauthorized access (Sipponen, 2022). The 1980s witnessed the emergence of the first computer viruses, such as the "Elk Cloner" and the "Brain" virus, malicious software that spread via infected storage media (Watson, 2022). This era highlighted the growing need for defensive technologies. In 1988, the Morris Worm incident marked one of the first significant internet-based attacks, infecting thousands of systems and underscoring vulnerabilities in network protocols (Shemakov, 2025). In response, the CERT (Computer Emergency Response Team) was recognised to co-ordinate responses to cybersecurity risks, a model that remains globally today.

2.2.1.2 Milestone in Cybersecurity Research & Practices

Cybersecurity risks increased significantly in the 1990s as a result of the internet's explosive growth. Firewalls, antivirus software, and intrusion detection systems (IDS) were also commonly utilized during this time (Aslan et al., 2023). Based on Li et al. (2023), this decade also saw the creation of numerous significant academic and industry forums focused on information security, such as the IEEE Symposium on Security and Privacy and the USENIX Security Symposium. Advanced malware operations such as Stuxnet (2010) emerged in the

early 2000s, targeting Iranian nuclear facilities, APTs, and state-sponsored cyber-espionage by exploiting zero-day vulnerabilities within Siemens SCADA (Supervisory Control and Data Acquisition) systems (Utinková, 2021). This attack demonstrated that, beyond its earlier theoretical discussion, cyberwarfare has turned into a strategic reality with real-world applications.

Also, the standardization of cybersecurity authority and risk management procedures was significantly improved by the announcement of frameworks like NIST's Cybersecurity Framework and ISO/IEC 27001 (Folorunso et al., 2024). These frameworks provide methodical conducts to assess and strengthen a business's cybersecurity position. In order to improve risk detection and mitigation abilities, cybersecurity research has extended in past years to take in AI, ML, and blockchain technologies. Furthermore, new study fields have developed to address the distributed nature and dynamic attack surfaces of contemporary digital ecosystems as a result of the growth of cloud computing, the IoT, and edge computing (Folorunso et al., 2024).

2.2.2 Core Concepts

2.2.2.1 CIA (Confidentiality, Integrity & Availability) Triad

The CIA Triad, which stands for three fundamental objectives that every information security plan must maintain, continues to be the foundation of cybersecurity principles:

- **Confidentiality**

Confidentiality guarantees that only authorized personnel can access sensitive information. Confidentiality is maintained by employing strategies including data classification, access limits, and encryption (Khanna, 2025). For instance, by encrypting communications between endpoints, Transport Layer Security (TLS) protocols protect data while it is in transit.

- **Integrity**

The accuracy and comprehensiveness of information are referred to as integrity. To identify unwanted changes, techniques like digital signatures, hashing algorithms (like SHA-256), and checksums are used (HIZA, 2022). Data integrity is crucial in financial systems because even small changes to transactional data can have big repercussions.

- **Availability**

Availability ensures that when authorized users need them, they can access systems and information. DoS attacks overload network resources, posing a direct threat to availability (Khanna, 2025). Plans for disaster recovery, load balancing, and redundancy are strategic actions to guarantee system resilience and uptime.

A triadic model comprising these three elements can jeopardize the security posture as a whole if any one of its components fails. For example, a ransomware assault can compromise confidentiality and integrity if data is exfiltrated, in addition to interfering with availability by encrypting files.

2.2.2.2 Comparing Threat, Vulnerability & Risk

For a cybersecurity risk assessment to be thorough, it is essential to comprehend the differences between risk, threat, and vulnerability.

- **Threat**

A potential source of an undesirable event that could endanger a system or enterprise is called a threat. Threats might be unintended (like natural disasters or human error) or intentional (like insider threats or hackers) (Landoll, 2021). A phishing email, for instance, is a threat vector designed to compromise user credentials.

- **Vulnerability**

A vulnerability represents a flaw or opening in a system that a threat could take advantage of. A poorly configured server, unpatched software, or ineffective authentication methods could be the cause of this (Milousi et al., 2024). A well-known vulnerability discovered in the Apache Struts framework, which had not been fixed, led to the notorious Equifax data leak in 2017.

- **Risk**

Risk is the possibility of suffering damage or loss as a result of a threat taking advantage of a weakness. It is frequently measured in relation to the impact and probability of a dangerous event (Landoll, 2021). Risks are systematically assessed and prioritized with the aid of risk management frameworks such as NIST SP 800-30 and FAIR (Factor Analysis of Information Risk).

In cybersecurity, risk management is locating vulnerabilities, assessing threats, and putting controls in place to lessen the possible damage. This helps to match security measures with company goals.

2.2.3 Cybersecurity Challenges in the Digital Age

2.2.3.1.1 Degree of Attack Complexity

A growing level of sophistication in adversary tools and strategies characterizes the current threat landscape. APTs are long-term, focused attacks that are usually planned by organized crime syndicates or state actors (Burita, & Le, 2021). These threats frequently use multi-stage attack chains, lateral network movement, zero-day exploits, and social engineering to evade detection. For instance, the 2020 SolarWinds Orion supply chain hack illustrated the breadth and depth of modern cyber-espionage (Cordey, 2023). Malicious code was inserted by threat actors inside genuine software upgrades, impacting hundreds of companies worldwide, including federal institutions in the United States (Krasner, 2021). To avoid detection by traditional approaches, the attackers employed stealth tactics like signed binaries and command-and-control servers that were masked as genuine communications.

Furthermore, cyberattacks are increasingly utilizing AI and machine learning. Cybercriminals can currently develop polymorphic spyware that alters its signature to evade detection by antivirus software, automate phishing attempts, and utilize deepfakes to mimic executives in audio or video forms (Khan et al., 2024). Attackers and defenders are engaged in an arms race that calls into question established security paradigms and demands proactive, flexible defences.

2.2.3.1.2 Digitization Increases Attack Surfaces

Every industry has seen a major increase in the attack surface due to digitization. Numerous opportunities for potential exploitation are presented by the use of cloud services, IoT, mobile platforms, and remote work infrastructures.

- **Cloud Computing**

While cloud computing has revolutionized IT operations, it also poses problems with shared responsibility models, data sovereignty, and improperly configured cloud storage (such as open S3 buckets). The 2019 Capital One hack stole more than 100 million customer details by taking advantage of a firewall that was improperly set (Khan et al., 2022).

- **Internet of Things**

From industrial control systems to smart thermostats, standardized security protocols are frequently absent from IoT devices, which include everything. Since these devices are usually installed with default login credentials, few firmware upgrades, and insecure communication protocols, botnets such as Mirai, which planned a large DDoS attack in 2016, target them (Bansal et al. 2022).

- **Remote Work**

The COVID-19 epidemic, which prompted remote work, has made security even more complex. Inadequate VPN setups, personal devices, and unprotected home networks have created additional avenues for unwanted access and credential theft (Aloisi, & De Stefano, 2022).

The combination of information technology (IT) and operational technology (OT) in critical infrastructure and smart manufacturing increases hazards since previously air-gapped devices are now internet-connected, frequently without proper security hardening.

2.3 Overview of Emerging Technologies

Emerging technologies are bringing forward new paradigms in data processing, communication, and computing that significantly alter the digital world. Even though these developments have enormous potential for a variety of sectors, including healthcare, banking, and national security, they also bring with them new cybersecurity threats (Angel et al., 2021). A thorough risk assessment in the modern cybersecurity space requires an understanding of the unique features, applications, and related vulnerabilities of these technologies.

2.3.1 Artificial Intelligence & Machine Learning

The term "artificial intelligence" was first used in 1956 by a Dartmouth workshop headed by Minsky and McCarthy. Later, it incorporated contributions from a wide range of research fields, including programming and computer science, robotics, neuroscience, philosophy, linguistics, and futurology (Negnevitsky, 2024). Although there is a lack of clarity in the vocabulary across disciplines, Rai (2024) offers a thorough review, even within the IS area, where definitions vary greatly. According to recent definitions, AI involves the entire concept of human intelligence and refers to a machine's capacity to carry out cognitive tasks that we associate with human minds, including perception, reasoning, learning, interaction with the environment, decision

making, problem solving, and even displaying creativity (Bhutani, & Sanaria, 2023). On the other hand, according to several experts, ML is a (sole) component of artificial intelligence. In the words of van Assen et al. (2022), learning is a fundamental aspect of human cognition. In order to better comprehend incoming input, humans use abstract knowledge to digest a large amount of data. The adaptive nature of machine learning models allows them to replicate human cognitive capacities (Rojas, 2024). As defined by Sarker (2021), machine learning refers to a collection of techniques that are frequently used to address a range of real-world issues with the aid of computer systems that are capable of learning to solve problems rather than having been manually programmed to do so.

Infrastructures for cybersecurity are rapidly incorporating AI and ML to improve threat detection, automate incident response, and forecast hostile behavior (Tanikonda et al., 2022). Network traffic anomaly detection, banking system fraud detection, and biometric authentication systems using facial recognition are examples of use cases. For instance, instead of depending on conventional signature-based detection, machine learning techniques are used to discover zero-day malware by examining behavioral patterns. However, there are a number of security considerations when using AI/ML (El Husseini et al., 2024). The vulnerability of machine learning models to adversarial assaults, in which inputs are purposefully constructed to trick the model, is one of the main issues. Adversaries can present minute alarms that evade detection to take advantage of mistakes in image recognition systems or interruption detection models (Tanikonda et al., 2022). In autonomous systems such as self-driving cars, in which inappropriate traffic sign classification by adversarial examples can result in disastrous failures, this is particularly decisive.

Data poisoning, in which attackers modify the training data required to create ML models, is another potential risk. The learning process can be contaminated by poisoned data, producing defective or negative results (Goldblum et al. 2022). In applications related to cybersecurity, this might make threat detection methods biased or ineffective. The inability to audit and articulate judgments is further hindered by the opaqueness of AI models, which is also referred to as the "black box" problem (Schnitzer & Tiruwuha, 2024). The lack of transparency creates problems for forensics and regulations, particularly in industries like healthcare and banking that require responsibility.

2.3.2 Internet of Things

The IOT concept was first introduced by a member of the Radio Frequency Identification (RFID) development community in 1999 (Mezzanotte et al., 2021). The proliferation of mobile devices, embedded and ubiquitous communication, cloud computing, and data analytics has made it more applicable to the real world in recent years. The term "Internet of Things" refers to the broad concept of objects, particularly commonplace ones, that can be read, identified, located, addressed by information-sensing devices, and/or controlled online, regardless of the media used for communication (e.g., RFID, wide area networks, wireless LAN, or other systems) (Akmal, 2021). The term "everyday objects" refers to not only the electronic gadgets we use or the products of advanced technology, like cars and machinery, but also items that we do not typically consider to be electronic, like food, clothing, chairs, trees, water, and so on (Akmal, 2021). Applications include wearables for healthcare, smart cities, smart homes, and industrial automation (Industrial IoT). According to Shafiq et al., (2022), there are presently over 15 billion IoT devices in use, and this number is only going to increase rapidly. The attack surface has been greatly expanded by the growth of IoT devices. Because many IoT devices have low memory and computing capacity, it is unable to implement strong security protocols like multi-factor authentication or strong encryption.

Their vulnerability is further increased by hardcoded credentials, default configurations, and incomplete firmware updates. Physical tampering is an actual risk vector since IoT devices are frequently placed in insecure settings and may be used unsupervised. For example, in the 2016 Mirai botnet assault, one of the biggest DDoS attacks ever was orchestrated by hackers using IP camera and router passwords that were deemed weak (Almazarqi, 2024). Vulnerabilities in inter-device communication are another serious issue. The proprietary communication protocols used by many IoT ecosystems might not be adequately encrypted or authenticated. In mesh networks, lateral mobility and complete network compromise are made possible by the compromise of a single device. Furthermore, attacks against SCADA systems in the context of the Industrial Internet of Things (IIoT) may physically interrupt key infrastructure or industry (Knapp, 2024). To ensure secure deployment and lifecycle management, the heterogeneity of devices and suppliers, along with the absence of defined security frameworks for IoT, pose significant hurdles.

2.3.3 Blockchain Technology

Typically, as per Neisser (1967), blockchain technology is linked to digital currencies like Bitcoin. It is a distributed database of transaction records that are kept up to date and verified by a global information network of computers (Faturahman et al., 2021). A vast community oversees the records rather than a single centralized body like a bank, and no one person has complete control over them. Additionally, no one can go back in time and alter or remove a transaction history. In contrast to a traditional centralized database, the distributed structure of blockchain technology and peer-confirmed guarantees prevent information manipulation (Faturahman et al., 2021). Blockchain technology is praised for its promise of immutability, transparency, and decentralization. Fundamentally, distributed consensus algorithms are used by blockchain to verify transactions over a decentralized network, which prevents manipulation and single points of failure. Digital signatures and hash chaining are two cryptographic techniques that guarantee the validity and integrity of data. Use cases include supply chain provenance, smart contracts, cryptocurrencies (like Ethereum and Bitcoin), and safe identity management (Al-Farsi et al., 2021). Theoretically, because blockchains are decentralized, they can withstand attacks like insider threats and database tampering. Nevertheless, this technology has a number of serious drawbacks and is not always safe.

The 51 percent attack, in which a malevolent player seizes most of a network's processing capacity, is one prominent weakness that allows them to change the transaction history or double-spend coins (Decker, 2025). Even for well-known blockchains, this is still a conceptual danger, even though it is more practical in lesser-known blockchains with less processing power. If smart contracts, self-executing code stored on the blockchain, are not properly developed, they can be exploited. The DAO hack of 2016 stole 60 million dollars in Ether by taking advantage of a recursive calling vulnerability within an Ethereum smart contract (Scharfman, 2024). Furthermore, user privacy is restricted even though transactions are unchangeable. Instead of providing complete anonymity, the majority of public blockchains provide pseudonymity. By analyzing patterns or addressing clusters, skilled attackers can de-anonymize people. Furthermore, one major weakness is still key management. Private keys that are lost or stolen may cause unlawful transactions or an irreversible loss of access (Decker, 2025). Finally, companies may choose to use centralized or hybrid models as a result of blockchain scaling

problems like latency and throughput. This partially eliminates the advantages of decentralized security and adds conventional potential risks relating to centralized systems.

2.3.4 Cloud Computing

Cloud computing has been described by IT industry leaders based on their own business viewpoints. Cloud computing, as reported by the US NIST, is a model that allows for easy, on-demand network accessibility to a shared pool of reconfigurable computing resources (such as networks, servers, storage, applications, and services) that can be quickly provided and released with little management work or service provider interaction (Al-Dulaimy et al., 2024). According to Lakshmi, & Tyagi (2024), computing is the foundation for the upcoming business generation. The entire stack of the IT industry is changing due to cloud computing: the hardware model, which delivers extremely powerful and efficient hardware at barely any of the cost; the application model, which enables developers to quickly develop highly responsive and secure cloud applications; and the operations model, which maintains cloud applications available around-the-clock with 9 to 5 management (Al-Dulaimy et al., 2024). Cloud computing offers scalability, cost-effectiveness, and operational flexibility by facilitating on-demand access to computer resources through the internet. Infrastructure as a Service (IaaS) and Software as a Service (SaaS) are examples of service models, whereas private, public, hybrid, and community clouds are examples of deployment models (Wulf et al., 2021).

Cloud computing increases company agility, but it also brings with it complicated cybersecurity issues, especially with regard to data protection and the responsibility-sharing paradigm (Lakshmi, & Tyagi, 2024). In this arrangement, customers are in charge of protecting their apps, data, and user access, while cloud providers are usually in charge of protecting the infrastructure. Inadequate knowledge or disregard for this divide frequently leads to security breaches. A prevalent issue is improperly set up cloud storage services, including publicly accessible Amazon S3 buckets. Millions of records have been compromised as a result of these settings errors, including private information (Baviskar, 2022). Furthermore, multi-tenancy in public clouds, particularly in virtualized systems, poses questions about side-channel attacks and data separation. Data processing and storage must adhere to stringent data privacy laws like the General Data Protection Regulation (GDPR) (Baviskar, 2022). Even when data is kept in

different jurisdictions, cloud clients still need to maintain compliance, which makes their legal and regulatory responsibilities more difficult.

Risks may include inadequate identity and access management (IAM) configurations and insider threats. Service interruption or extensive data exfiltration may result from a hacked administrator account (Wulf et al., 2021). Although cloud providers provide security monitoring, audit logging, and encryption tools, customers are still responsible for properly configuring and keeping an eye on these measures.

2.3.5 Quantum Computing

Quantum computing, as stated by Tarlaci, (2022)), represents an entirely new type of computing that has its foundation on quantum mechanics and addresses the probabilistic and unpredictable physical reality. Since quantum mechanics is a more universal framework for physics than classical mechanics, it leads to a more universal model of computing, known as quantum computing, which has the capacity to address issues that classical methods are unable to. They employ their own quantum bits, sometimes known as "Qubits," for storing and manipulating the data, in contrast to other classical computers that rely on conventional computing, which uses binary bits 0 and 1 separately (Zhu et al., 2023). These kinds of computers are referred to as "Quantum Computers." Circuits containing integrated circuits, logic gates, and transistors are not feasible in such tiny computers. By taking advantage of the concepts of quantum physics, particularly superposition and entanglement, quantum computing is a significant paradigm shift in computing capabilities that allows for substantially quicker computations than traditional computers (Rascão, 2024). Despite being in the early stages of development, it has the potential to have a significant impact on cybersecurity and should be given thoughtful consideration.

It can defeat modern cryptographic techniques, especially ones that rely on asymmetric encryption, which is the primary root of concern. For instance, Shor's algorithm has the ability to factor big prime numbers effectively, endangering the security of RSA, ECC (Elliptic Curve Cryptography), and DH (Diffie-Hellman) algorithms, which are the foundation of digital signatures, blockchain, and secure web communications (Dalal et al., 2024). Although not as much, symmetric encryption is also threatened by quantum computing. With Grover's technique, symmetric algorithms such as AES can have their effective security cut in half, requiring the usage of greater key lengths. As a result, post-quantum cryptography (PQC), which focuses on

creating algorithms that are resistant to quantum errors, has arisen (Mamatha et al., 2024). Standardization of such algorithms is presently underway at the NIST in anticipation of the quantum risk. From a strategic point of view, the idea of "harvest now, decrypt later" is becoming more popular. When quantum capabilities become practical, adversaries may collect encrypted data today with the goal of decrypting it (Dalal et al., 2024), potentially exposing private information long after it has been transmitted. This reinforces the requirement for quantum-safe cryptographic transitions and forward-looking encryption techniques.

2.3.6 Integration of Emerging Technology

While there is unique cybersecurity risks associated with each developing technology, the risks are increased and frequently unforeseen when these technologies are integrated into larger networks. The vulnerabilities of each of the domains are encapsulated in AI-powered IoT systems that are deployed on cloud infrastructure, for example, and could result in a single point of failure that has a significant impact (Dhayanidhi, 2022). Consider intelligent healthcare settings where wearable IoT devices track patient vitals and provide data to cloud platforms for diagnostics powered by AI. A vulnerability in such a system can affect diagnostic algorithms (model integrity), interfere with service availability (critical care), and jeopardize patient confidentiality (data privacy) (Areo, 2024). Although they all need different security frameworks, the device, network, data processing, and analytics layers must work together.

Furthermore, interdependencies have the potential to spread vulnerabilities. A misconfigured cloud resource might allow ML training datasets to be tampered with, or a flaw in an AI model could be used to change how blockchain-based smart contracts are executed (Shah et al., 2023). Additionally, integration expands the attack surface and attack routes, making multi-layered protection systems and cross-domain threat modelling necessary. This technological convergence necessitates interdisciplinary cybersecurity strategies that combine knowledge of system design, data science, cryptography, and regulatory compliance (Qudus, 2025). The linear models utilized in risk assessments must also provide a way to complex, systems-based analyses that take dynamic risk situations and cascading outcomes into consideration.

2.4 Current State of Cybersecurity in Emerging Technologies

The integration of emerging technologies, such as IoT, blockchain technology, cloud computing, edge computing, and IIoT, has substantially redefined the cybersecurity landscape. While such

innovations quicken digital transformation and improve operational efficiency, they also present new layers of vulnerabilities that are integrally rooted in their protocols, structures, and deployment models. The current state of cybersecurity in these technologies exposes not only a proliferation of attack surfaces but also shortages in resource prioritization, risk modelling, and regulatory precision. In the field of IoT, Arora et al. (2024) projected a four-tiered framework of cyber risk management that categorizes risks into network-level, application-level, device-level, and user-level vulnerabilities. This tiered approach permits granular risk analysis, yet the authors underscore the absence of structured financial mechanisms to implement multi-layered protection. Insecure communication protocols (such as MQTT and CoAP) and low-power devices' lack of integrated encryption are especially worrisome since they leave IoT ecosystems vulnerable to unauthorized firmware updates, spoofing, and man-in-the-middle (MITM) attacks. The methodological framework recommends programmatic allocation of resources to high-risk layers, but it also points out that existing implementations frequently lack data-driven approaches to guide these decisions, which can result in important components being either over- or under-protected.

Risk is significantly increased by cloud technology. In cloud-native systems, where shared responsibility models generate uncertainty between supplier and consumer security requirements, Möller (2023) criticizes the NIST Cybersecurity Framework for being incapable of directing the cost-benefit prioritizing of security measures. For instance, misconfigured S3 buckets in Amazon Web Services (AWS) remain one of the most common causes of data leaks, despite available encryption tools, suggesting that awareness and procedural integration lag behind technical capability. Blockchain technology, despite being lauded for its immutable ledger, is not inherently secure in all components. Alfandi et al. (2021) underscore how smart contracts, once deployed, are immutable and publicly visible, making them prone to exploitation through logic errors and reentrancy attacks, as demonstrated in the infamous DAO hack on Ethereum. Their study explores countermeasures such as formal verification techniques, off-chain computation using Trusted Execution Environments (TEEs), and confidential transactions via zero-knowledge proofs. However, these solutions are either computationally expensive or not yet standardized, limiting their real-world applicability.

In edge computing, security challenges stem from the highly decentralized and resource-constrained nature of edge nodes. Bhushan et al. (2021) identify rogue edge nodes, latency-focused security trade-offs, and lack of federated identity management as key risks. They propose homomorphic encryption for data-at-rest, secure multi-party computation (SMPC), and blockchain-backed audit logs to maintain integrity and traceability. However, such methods often exceed the processing capabilities of edge hardware, making their deployment infeasible at scale without additional infrastructure. Goudarzi et al. (2022) highlight regulatory and institutional issues in securing FinTech, smart grids, and critical IoT infrastructures, noting that these sectors involve cross-domain jurisdictional challenges. Unlike legacy systems, emerging technologies often straddle multiple regulatory boundaries. For instance, FinTech applications must simultaneously adhere to financial, data protection, and cybersecurity regulations across jurisdictions, making compliance fragmented and inconsistent. Consequently, lawmakers increasingly defer to federal agencies to clarify boundaries and assign responsibility, leading to delays in enforcement and gaps in regulatory coverage, as also echoed by Alfandi et al. (2021).

To manage cybersecurity incidents across heterogeneous environments, Security Information and Event Management (SIEM) systems offer centralized monitoring and correlation capabilities. Sania et al. (2024) highlight SIEM tools' ability to detect lateral movement, standardize log formats from disparate sources, and identify early-stage APTs, particularly in Smart Grid infrastructures. They support AI-driven SIEM improvements that may identify abnormalities and understand baseline activity patterns, especially when attackers employ low-and-slow strategies to avoid conventional detection. Mekala et al.'s (2023) investigation of the cybersecurity status of IIoT systems in industrial contexts notes that OT frequently lacks the segmentation tactics and patching processes found in IT systems. They concentrate on ML-based predictive security algorithms that predict harmful activities by discovering time-series anomalies. However, there are still issues with training reliable machine learning models on asymmetrical or unstructured industrial datasets, which can result in significant false-negative or false-positive rates.

Emerging technological uses in healthcare raise unique issues. In their analysis of the Internet of Medical Things (IoMT), Razdan and Sharma (2022) describe how faulty authentication systems, non-standard device firmware, and Bluetooth Low Energy (BLE) vulnerabilities might result in direct patient injury or data breach. Their research suggests blockchain-based consent

management systems, biometric authentication, and device attestation protocols as ways to strengthen accountability and trust, particularly in telemedicine and remote monitoring applications. When taken as a whole, these studies show that the cybersecurity safeguards in place for new technologies are disjointed, poorly executed, and frequently reactive. Security architectures that are context-aware, scalable, and consistent with regulations and that are adapted to the distinct threat environments that each technology presents are conspicuously lacking. Moreover, the lack of harmonized international standards, coupled with varying levels of technological maturity, exacerbates the complexity of developing unified cybersecurity protocols. The reliance on traditional tools and frameworks, in many cases, does not translate into adequate security posture in the face of AI-generated exploits, zero-day vulnerabilities in decentralized systems, or supply-chain attacks in cloud environments.

2.5 Cybersecurity Risks in Emerging Technologies

2.5.1 Threat Landscape

The extent and sophistication of the threat landscape have increased dramatically in the context of emerging technologies. As businesses incorporate more disruptive technologies into their infrastructures, the attack surface grows rapidly. Because of this, there are new vulnerabilities that conventional security paradigms cannot address (Lehto, 2022). To evaluate the cybersecurity threats posed by developing technologies, a more thorough understanding of the main threat vectors, such as ransomware, malware, phishing, and zero-day exploits, as along with state-sponsored and APTs, is extremely important.

2.5.1.1 Phishing Attack in *Emerging Platforms*

Although phishing attacks are still one of the most common risks on the web, their methods have changed to target cloud services, chatbots powered by artificial intelligence, and remote collaboration platforms. In cloud settings like Google Cloud Platform and Microsoft Azure, attackers are increasingly imitating official identity providers or OAuth authentication screens in order to obtain credentials (Di Federico & Barcaroli, 2022). By taking advantage of token-based access systems, this kind of credential phishing can rarely avoid multi-factor authentication (MFA) (Muir et al., 2024). Besides, by contextually and accurately imitating natural language, AI-driven material is often used by phishing campaigns to modify email attacks, improving their success rate.

Phishing is correspondingly increasingly being used in the early stages of larger attacks, such as the release of lateral movement or ransomware in hybrid IT infrastructures. For example, a malicious document within a phishing email can operate scripts to raise privileges, generate persistence on a computing device, and grant remote access for more exploitation. Living-off-the-land binaries (LOLBins) are a way to further hide the attack chain by employing trusted system utilities to evade detection (Ning et al., 2023).

2.5.1.2 Malware Targeting in Emerging Technology

Malware has changed from being signature-based and generic to becoming context-aware, polymorphic, and more autonomous as a result of AI integration. Within the Internet of Things, malware like Mirai, Mozi, and Hajime take advantage of exposed Telnet ports and default credentials on devices like industrial sensors, thermostats, and smart cameras (Zhang, 2022). In order to carry out enormous DDoS attacks, these attackers seek to integrate devices into botnets. The issue is made more serious by IoT devices' intrinsic hardware limitations, which restrict the use of endpoint security tools like runtime behavioral monitoring and anti-malware software.

Malware can also affect AI systems. In order to distort machine learning models' ability to make decisions, skilled attackers may introduce data poisoning into training datasets. This approach jeopardizes the fundamental integrity of the AI system (Yerlikaya & Bahtiyar, 2022). Furthermore, by facilitating automated decision-making to avoid sandboxes or honeypots and real-time environmental analysis, AI can be abused to improve malware capabilities. Due to their spatial dispersion, malware can infiltrate distributed edge nodes in developing fields like edge computing to carry out decentralized (Yerlikaya & Bahtiyar, 2022), persistent attacks that are more difficult to detect and counter.

2.5.1.3 Ransomware in Environments with High Availability

Attacks using ransomware have become increasingly calculated, focusing on sectors that depend heavily on operational continuity and uptime. Smart manufacturing, energy, healthcare, and financial services are especially vulnerable (Möller, 2023). With the emergence of Industry 4.0 and the implementation of IIoT systems, ransomware has given attackers the power to stop entire production processes. For instance, the 2021 assault on Colonial Pipeline exposed the susceptibility of OT settings to ransomware threats and impacted fuel transportation throughout the U.S. East Coast (Rahman, 2025), despite coming from compromised credentials.

In order to carry out double-extortion schemes, modern ransomware versions such as Ryuk, Conti, and LockBit use lateral movement tactics, Active Directory enumeration, and even data exfiltration (Ahmed, 2024). If ransom demands are not fulfilled, victims are threatened with the release of their data to the public. Because ransomware-as-a-service (RaaS) models have been adopted, attackers now have easier access to advanced attack tools (Alwashali et al. 2021), which has increased the threat of ransomware.

2.5.1.4 Zero-Day Attacks on Undeveloped Technologies

One of the most serious risks in the field of cybersecurity is the existence of zero-day vulnerabilities, especially when they are present in emerging technologies that have not yet undergone thorough security testing (Williams, 2021). Adversaries have a crucial time advantage because these vulnerabilities are used before the vendor is aware of them or has patched them. For example, in 2021, more than 30,000 companies globally, many of which had just made the switch to hybrid cloud environments, were compromised by a zero-day in Microsoft Exchange Server (called ProxyLogon) (Mesiä, 2024).

Zero-day vulnerabilities in blockchain platforms can appear as smart contract issues, which allow bitcoin to be stolen by taking advantage of holes in the logic of decentralized applications (dApps) (Erinle et al., 2023). Likewise, zero-day-like attacks on AI models can include membership inference or model inversion, in which adversaries use the algorithm's outputs to recreate private training data. These methods have significant effects on the privacy and secrecy of systems that use personalized AI or federated learning.

2.5.1.5 APTs & State-Sponsored

APTs and state-sponsored assaults are members of a high-level threat category that is long-term, strategic, and frequently clandestine. In contrast to traditional cybercriminals who are motivated by financial gain, APTs are motivated by economic, military, or geopolitical objectives (Mancuso, 2023). They target pharmaceutical corporations, defense contractors, national infrastructure, and up-and-coming technological companies.

Groups including Charming Kitten, Lazarus Group, APT29 (Cozy Bear), and APT28 (Fancy Bear) have been linked to campaigns that steal intellectual property associated with semiconductor designs, AI algorithms, vaccine research, and quantum computing developments (Saalbach, 2024). These attacks usually start with advanced spear-phishing emails, and then they

use backdoors, specialized malware toolkits, and command-and-control (C2) infrastructure that is made to be persistent and stealthy.

The way that APTs take advantage of vulnerabilities in the supply chain is one of their distinguishing characteristics. One well-known example is the 2020 SolarWinds breach, in which hackers introduced malicious code into a regular software update that impacted hundreds of firms globally, including government institutions in the US (Alkhadra et al., 2021). In the context of developing technologies, cloud-native apps, IoT firmware updates, and pipelines for distributing AI models might all use this strategy.

2.5.2 Vulnerabilities in Emerging Technologies

Industries are being revolutionized by emerging technology, but they additionally carry with them new and frequently neglected risks. These vulnerabilities, which originate from the architectures, deployment methods, and operational settings of the technologies themselves, are frequently inherent to the technologies themselves rather than being merely extensions of conventional security flaws (George & George, 2024). Three major types of vulnerabilities in emerging technologies are examined in this section: adversarial threats to AI systems, such as model poisoning; smart contract defects in blockchain platforms; and unsecured Application Programming Interfaces (APIs) in IoT systems.

2.5.2.1 Insecure APIs in IoT Environments

The proliferation of badly designed or unsafe APIs, which are dynamic interfaces for communication between users, platforms, and devices, is one of the most extensive risks in IoT ecosystems (Teuguia, 2025). IoT architectures, contrary to typical business systems, occasionally rely on trademarked APIs and inconsequential protocols that are inadequately protected due to limitations on storage, energy, and processing capacity.

These APIs often lack important security features like encryption, input validation, authorization, and authentication, which leaves them exposed to attacks like MITM, replay attacks, and API enumeration. For example, the 2018 Insecam platform attack revealed a widespread lack of access control within consumer IoT installations by providing unauthorized users with unprotected APIs that let them to access thousands of IP cameras worldwide (Anderson et al., 2021).

2.5.2.2 Smart Contract Vulnerabilities in Blockchain Platforms

Cryptographic assurance, blockchain technology, decentralization, and immutability are frequently commended for their security advantages. However, the application layer has serious security concerns, namely with regard to smart contracts. On blockchain networks such as Ethereum, smart contracts are self-executing programs that automate transactions without the need for intermediaries (Toheeb et al., 2025). Their immutability, however, also makes any vulnerabilities or defects present upon placement irreversibly exploitable.

Integer overflows and underflows, reentrancy attacks, front-running, and logical mistakes are cases of common smart contract vulnerabilities. One standard example is the notorious DAO hack in 2016, in which an invader recursively exhausted over 60 million US dollars' worth of Ether out of the regionalized investment fund to exploit a reentrancy vulnerability (Tsai et al., 2023). The exploit was able to take place prior to the updating of balances since the smart contract lacked the necessary state-update methods.

2.5.2.3 AI Model Poisoning & Adversarial Attacks

A distinct set of vulnerabilities that are essentially different from those of traditional software are introduced by artificial intelligence, especially ML and deep learning systems. These comprise inference-time attacks like adversarial examples and training-time attacks like model poisoning. These assaults, which are frequently missed by standard security measures, alter the statistical structure of AI models in contrast to more common buffer overflows or SQL injections (Augustine et al., 2024).

In model poisoning, also known as data poisoning, malicious or deceptive data is purposefully added to the training dataset. When AI models are trained on tainted datasets, the attacker can include backdoors that act maliciously under certain inputs or subtly impair model performance, particularly in federated learning or open-source environments (Wan et al., 2024). For instance, the model might incorrectly categorize stop signs in a poisoned picture dataset for driverless cars, which could have disastrous real-world repercussions.

Inference is similarly vulnerable to adversarial attacks. These techniques manipulate inputs such that AI models incorrectly classify them even while they seem normal to human observers. An attacker could, for example, tamper with an image to make a computer vision model identify a "banana" as a "toaster," jeopardizing object recognition systems like drones, driverless cars, or

surveillance systems. The Fast Gradient Sign Method (FGSM), a popular technique, uses model gradients to calculate minimum perturbations that can highly confidently mislead a neural network (Naseem, 2024).

2.6 Challenges in Managing Risks in Emerging Technologies

Organizations are becoming more and more concerned with tackling cybersecurity risks associated with emerging technologies in the rapidly evolving world of technology. The challenges include organizational, technical, and regulatory aspects that are intricately linked. Innovations in technology like cloud computing, AI, and the IoT are definitely revolutionary (Jimmy, 2021). They do, however, also introduce fresh vulnerabilities that need to be fixed. The necessity for organizations to proactively secure devices while safeguarding data in order to foresee the risks associated with developing technologies has been made evident by recent instances. Given how dynamic these technologies are, timely threat intelligence and ongoing monitoring are essential. On the other hand, the lack of qualified cybersecurity experts who can adjust to the developing environment is a major issue that organizations must address. Organizations must establish a widespread cybersecurity culture in addition to hiring (Jimmy, 2021). This involves setting in place complex training programs, awareness campaigns, and cultivating a feeling of shared accountability for cyber resilience.

Regulatory issues pose a special challenge. Regulatory frameworks find it difficult to keep up with the rapid advancements in technology, which results in gaps that breed uncertainty. The complicated requirements that organizations must manage are highlighted by recent debates on privacy and data protection laws (Akpobome, 2024). A sensitive issue that organizations must aim to accomplish is striking a balance between compliance and the flexibility to adapt to new regulatory changes. All three of these challenges are interconnected, which makes the technical environment more complex and increases the difficulties that organizations and regulators face. It is essential to maintain privacy standards, device security, and the management of extensive ecosystems while adhering to constantly shifting legal requirements (Akpobome, 2024). Organizational and technical aspects are intertwined with regulatory challenges. Uncertainties arise from holes in regulatory frameworks caused by technology exceeding them. A complicated task with organizational and technical components is striking a balance between agility and compliance in the face of changing requirements.

2.6.1 Organizational Challenges

For organizations, managing the risks related to cybersecurity in emerging technology presents challenges that must be resolved. The culture and awareness of talent management are among these challenges (Safitra et al., 2023). When it involves mitigating cybersecurity risks, talent management presents a unique administrative challenge. The COVID-19 pandemic has expedited the shift to virtual workplace environments, which has made cybersecurity risk management more difficult (Aloisi, & De Stefano, 2022). Organizations need to understand the complexities of managing cybersecurity teams. Ascertain that they have the necessary skills to address new risks. To effectively manage and reduce the risks connected to emerging technologies, this requires hiring and keeping cybersecurity experts (Safitra et al., 2023).

Yet another significant challenge facing the company is developing a cybersecurity culture. Historically, using controls like software and hardware systems has been crucial to safeguarding information assets. However, in the face of contemporary information risk situations, protection alone is not enough. An organization's cybersecurity culture encompasses its people, procedures, guidelines, symbols, technology, education, expertise, commitment, and concrete measures to ensure cybersecurity (De Silva, 2023). In order to create a cybersecurity culture, it is necessary to raise employee knowledge through training programs and to encourage a sense of accountability and dedication to upholding security protocols.

Additionally, it is still critical to raise awareness of cybersecurity risks. Managers and legislators are reevaluating cybersecurity measures at organizational, sectoral, and national levels as a result of the growing severity of cyber threats (Tsohou et al., 2023). Organizations must be aware of potential cyberthreats and the effects that data breaches may have on their business operations (Naik, 2022). With this insight, businesses may create plans and take steps to lower cybersecurity threats.

Meanwhile, the intricacy of cybersecurity management in a hybrid or multi-cloud IT environment places a heavy burden on organizational capability. It is becoming increasingly difficult to manage heterogeneous infrastructures with varying security standards as more businesses integrate IoT devices and embrace cloud-native technologies. As stated by Zhou and Buyya (2021), IT departments must now keep an eye on real-time data flows, spot platform irregularities, and implement uniform security governance even when there are different cloud

providers and operational frameworks. There may be policy gaps, configuration errors, and heightened susceptibility to lateral movement assaults if such settings are not harmonized.

The management of emerging technologies that violate legal requirements is another important issue. Blockchain-enabled contracts and AI-driven analytics are two examples of technologies that frequently develop more quickly than the institutional structures intended to oversee them, creating a compliance gap. Businesses operate in morally and legally uncertain territories where implementing new technologies may improve operations while also posing unknown concerns (Edwards, 2024). Therefore, it is crucial to set up internal governance systems that are able to proactively assess technical risks and apply flexible cybersecurity measures.

Finally, organizational preparedness continues to be restricted by the lack of specialist cybersecurity positions, especially in cloud security engineering, secure DevOps, and AI for cybersecurity. Many businesses lack the human capital necessary to contextualize risks, use threat modeling, or carry out advanced risk assessments in line with certain developing technologies, even as investment in security products is increasing (Edwards, 2024). In addition to hiring new employees, closing this talent gap calls for intentional workforce development through role-based upskilling programs, industry-academic partnerships, and certifications.

2.6.2 Technical Challenges

In order to effectively manage cybersecurity risks in emerging technologies, organizations must overcome a number of technical challenges. These challenges result from the complexity and dynamic nature of emerging technologies along with the growing sophistication of cyberthreats (Yaseen, 2024). The following sources shed light on the technological challenges involved in controlling cybersecurity threats in cutting-edge technologies. The rise of Fintech in the banking sector emphasizes the need for robust cybersecurity and anti-fraud protocols. Ng and Kwok (2017) state that among the technological challenges in safeguarding financial technology are protecting sensitive financial data, ensuring secure transactions, and thwarting cyberattacks which target financial institutions.

The swift incorporation of innovative technologies like Fintech, Smart Grids, and the IoT into vital infrastructure systems, particularly energy grids, has created difficult technical cybersecurity issues. Increasingly, power grids rely on distributed digital architectures, such as IoT-enabled smart meters, Supervisory Control and Data Acquisition (SCADA) systems, and

Advanced Metering Infrastructure (AMI), all of which are susceptible to cyber intrusion if not sufficiently secured (Olaiya et al., 2024). Due to their heterogeneous platform operation, these components have interoperability problems and are more vulnerable to data manipulation, denial-of-service assaults, and virus transmission. Abir et al. (2021) claim that while the decentralized structure of smart grids allows for two-way communication between businesses and customers, it also creates attack points for remotely adjusting load distribution, introducing fake data injection (FDI), and compromising control logic. In order to mitigate these risks, research is being done on anomaly-driven intrusion detection systems (IDS) that use machine learning, public key infrastructure (PKI), and fine-grained access control. According to Amoo et al. (2024), in order to guard against eavesdropping and unauthorized penetration in energy management systems, cloud-secured data transfer and dynamic authentication procedures are essential.

Additionally, another area of technological issue is vehicle cybersecurity. Because connected cars depend on vehicle-to-everything (V2X) communications and in-vehicle networks (CAN, LIN), vulnerabilities including MITM attacks, OTA firmware hijacking, and electronic control unit (ECU) spoofing present urgent safety risks (Rathore et al., 2022). safeguard boot procedures, real-time encryption methods, and hardware-based security modules must all be incorporated into the design process in order to safeguard automotive systems. Without these, hackers might jeopardize vital transportation infrastructure, physical safety, and digital systems. Table 3 provides a summary of the difficulties in addressing cybersecurity threats, independent of emerging technology.

Table 3: Technical Challenges in Emerging Technologies for Cybersecurity Risks

Emerging Technologies	Technical Challenges
Fintech	Safeguarding private financial information, Providing safe transactions, Protecting against online dangers
Power Grids	Protecting networks of communication, Security of control systems, Grid defense

	against online threats
IoT	Protecting networks of communication, Protecting control systems, Resilience of devices against cyberattacks
Cloud Computing	Protecting data and apps, Securing communication networks, Cloud service integrity and privacy
AL & ML	Protecting AI algorithms and models, Keeping training data safe, AI systems' dependability and integrity
Blockchain Technology	Safeguarding data and transactions, Securing communication networks, The dependability and integrity of blockchain networks
Quantum Computing	Protecting data and systems, Securing communication networks, Integrity and dependability of computing systems

2.6.3 Regulatory Challenges

The governance of cybersecurity in emerging technologies faces substantial regulatory challenges stemming from the complexity, novelty, and pace of innovation. As technologies continue to transform critical sectors, the inadequacy of traditional regulatory frameworks becomes increasingly apparent (Abikoye et al., 2024). These technologies often operate in decentralized, data-intensive environments, rendering conventional command-and-control legal models ineffective. A key regulatory challenge is the inability of national and international legislative systems to keep pace with the evolving threat landscape. For instance, blockchain-based applications, such as decentralized finance (DeFi), lack clear regulatory oversight due to their pseudonymous and borderless nature. Smart contracts, which execute autonomously, raise complex questions of liability and enforceability under existing civil and commercial law

(Siddique, 2022). Similarly, AI-driven cybersecurity tools, while efficient in anomaly detection, introduce regulatory concerns about algorithmic transparency, explainability, and unintended discrimination. There is no unified global protocol to audit or regulate AI systems deployed in sensitive infrastructures, further complicating compliance and accountability.

Compliance-related challenges are particularly burdensome for organizations implementing emerging technologies. Sectors such as banking must simultaneously adhere to the Payment Card Industry Data Security Standard (PCI DSS), Anti-Money Laundering (AML) directives, and evolving fintech-specific guidelines. In healthcare, integrating IoMT devices demands compliance with HIPAA, while also ensuring interoperability and real-time monitoring. In the opinion of Abikoye et al. (2024), these overlapping requirements necessitate ongoing risk assessments, reporting of incident procedures, and cryptographic protections capabilities that are frequently absent from underfunded organizations or new systems. In Malaysia, the Malaysian Communications and Multimedia Commission (MCMC) is in charge of regulatory oversight in accordance with the Personal Data Protection Act 2010 (PDPA) and the Communications and Multimedia Act 1998 (CMA). Although these statutes cover broad cybersecurity concepts and the protection of personal data, they do not address particular vulnerabilities resulting from the growth of IoT devices, blockchain immutability, or AI inference issues. For example, there is no advice on data leaking in AI-produced medical diagnostics or adversarial AI assaults in driverless cars (Mohamad et al., 2024). The prosecution and settlement of cyber events are made difficult by the lack of precise legal categories for these risks.

Another important challenge is international collaboration. Global cyber events like SolarWinds and Log4Shell have drawn attention to the necessity of coordinated response plans, although regulatory asymmetry between states still hinders cooperative defenses. The regulatory burden is made severe by disparate data residency guidelines that are contradictory to breach reporting deadlines, and uneven encryption standards, especially for global technology companies (Siddique, 2022).

2.7 Theoretical Framework

A solid theoretical foundation is required in order to guide research into cybersecurity threats associated with developing technologies. It offers a conceptual framework for comprehending how risk perception, user acceptability, and mitigation strategies interact with technical

innovation. Three well-known models are employed in this study: ***The Risk Management Framework (RMF)*** offers a scientific and systematic way to evaluate, put into practice, and continuously monitor security policies that are appropriate for various technological environments. The ***Technology Acceptance Model (TAM)*** is used to examine the cognitive and behavioral factors that affect stakeholders' readiness to embrace new technologies. The ***Diffusion of Innovation (DOI) theory*** is used to study the adoption and distribution of emerging technologies over time among various user groups.

2.7.1 The Risk Management Framework

The RMF was created by the NIST and offers a comprehensive and structured process for managing cybersecurity risks across information systems, especially those that support dynamic missions and commercial operations. The framework consists of six interrelated steps: (a) Information System Categorization; (b) Security Control Selection; (c) Security Control Implementation; (d) Security Control Assessment; (e) Information System Authorization; and (6) Security Control Monitoring (Kure et al., 2022). Because each step of the RMF is systematically designed to evaluate and reduce risks, it is very pertinent for assessing cybersecurity risk in developing technologies.

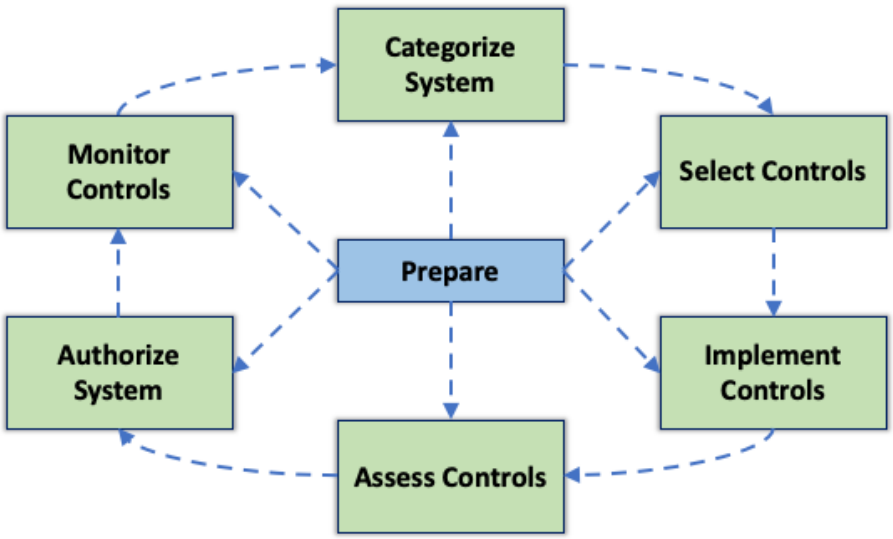


Figure 1: Risk Management Framework (RMF)

Within the realm of emerging technologies, the Risk Management Framework provides a theoretical framework for examining potential methods for risk forecasting, measurement, and mitigation in environments characterized by swift innovation and dynamic risk environments (Lee, 2021). These technologies are susceptible to a wider variety of risks, meanwhile, they usually function in highly organized, dynamic ecosystems. In this setting, the first step of the RMF, ***Categorize Information Systems***, becomes more important since it requires a contextual understanding of the operating environment and the influence level (low, moderate, or high) of an incident involving security (Alzoubaidi et al., 2023). For example, understanding the CIA requirements specific to patient data and real-time health telemetry is necessary to classify an IoT-based health monitoring system.

In evolving technology settings, the ***Selection and Implementation of Security Controls*** in accordance with RMF phases two and three are of equal significance. Specialized control baselines for technologies like cloud computing and industrial control systems are offered by NIST's SP 800-53 and SP 800-82 (Murino et al., 2021). Because emerging technologies have non-traditional architectures, they may require unique or hybrid control systems. Blockchain-based applications, for instance, might need new consensus protocol hardening or access control methods that current frameworks might not adequately handle (Kure et al., 2022). By allowing controls to be personalized to specific technology requirements, the RMF makes it possible to implement a risk mitigation plan that is more context-sensitive and efficient.

Since emerging technologies are continuously evolving, the ***Assessment of Security Controls*** (step four) is based on constant validation of a risk model that is focused on change. Through vulnerability study, penetration testing, and security evaluations, the RMF reassures a thorough analysis of control efficacy (Lee, 2021). AI-driven systems, for instance, are vulnerable to data poisoning, model inversion, and adversarial attacks, each of which requires the use of sophisticated risk assessment techniques. Through a systematic assessment of the controls planned to address these risks, RMF supports provide quantitative information on residual risk.

Additionally, while integrating novel technologies, the ***Authorization of Security Controls*** stage of the RMF becomes essential for determining accountability and assisting in informed decision-making (Alzoubaidi et al., 2023). System proprietors need to consider the trade-offs between risk and innovation, and the RMF provides a systematic framework for making these decisions

through credentials on risk acceptance and mitigation. Finally, the continuous ***Monitoring of Security Controls*** stage underlines how dynamic and continuous cybersecurity risk is, which is mainly relevant in new technology placements where user behavior, risk vectors, and system updates are continually altering (Murino et al., 2021). In line with RMF's aim of actual behavior analytics, risk management, SIEM systems, and automated compliance technologies are being implemented.

2.7.2 Technology Acceptance Model

In 1986, the TAM was developed by Davis and provides a behavioral theoretical framework for considering how individuals adopt and exploit technology. As stated by TAM, which has its origins in the ***Theory of Reasoned Action (TRA),*** two core factors, ***Perceived Usefulness (PU) and Perceived Ease of Use (PEOU)***, have an important effect on an individual's acceptance of a technology (Fakir, 2024). These factors directly influence the user's ***Attitude Toward Using (ATU)*** of the system, which sequentially impacts the ***Behavioral Intention to Use (BI)***, and eventually outcomes in the actual use of the system.

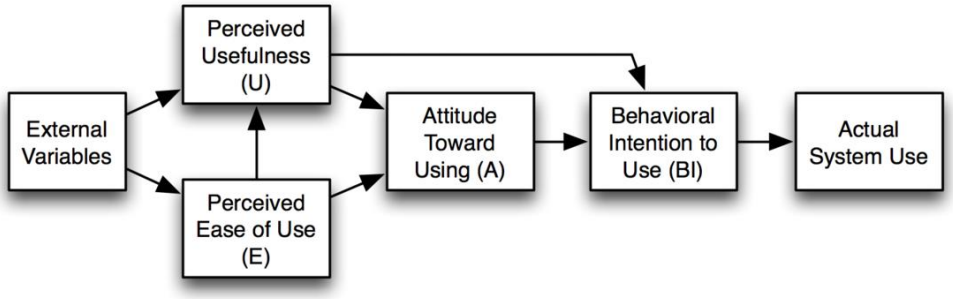


Figure 2: Technology Acceptance Model (TAM)

Within the setting of cybersecurity risk and emerging technologies, TAM provides an vital lens through which to interpret the human aspects of technology implementation and the risk behaviors that accompany it. While RMF concentrates on methodical risk management, TAM assists in placing stakeholders' perceptions and reactions to cybersecurity measures incorporated into new technologies in context, including end users, administrators, and decision-makers (AMRON, 2021). For example, users may be reluctant to embrace security procedures that are

included in IoT devices because they believe they are complicated or inconvenient, which raises the general risk profile for the technology deployment.

When businesses deploy security solutions for new technologies, ***perceived usefulness*** transforms into an important consideration (Fakir, 2024). Users are more inclined to embrace and follow security measures if they believe they will significantly enhance performance or safeguard private information. Examples of these measures include zero-trust architectures, two-factor authentication, and AI-based intrusion detection systems. On the other hand, low compliance could negate the technical efficacy of these procedures if they are perceived as restrictive (Ebot, 2024). In a blockchain setting, for instance, consumers may steer clear of private key storage apps if they believe they are overly complex, increasing their vulnerability to cyberattacks.

The probability that cybersecurity policies will be successfully implemented in developing tech environments is also influenced by ***perceived ease of use***. Usability issues may prevent emerging technologies from being effectively adopted as their interfaces and features become more complex. Research has indicated that even in high-risk settings, technologies with user-friendly interfaces and little friction are more inclined to be adopted (AMRON, 2021). For example, security analysts may not fully exploit an AI-driven anomaly identification dashboard that has poor visualization, even though it has the ability to offer real-time threat information.

Additionally, TAM has been expanded in a number of studies to incorporate concepts that are especially pertinent to cybersecurity research, such as perceived security and trust. Users of developing technologies frequently have to have faith in the security measures, data handling protocols, and infrastructure. For instance, users are concerned about location tracking and spying as a result of the rollout of 5G networks (Ebot, 2024). Regardless of the technology's apparent technological advantages, user adoption is less likely if it is not seen as secure. Researchers may systematically examine these impressions and compare them to actual usage patterns and compliance levels through the use of TAM.

TAM can be used in organizational contexts to comprehend how corporate users engage with cybersecurity governance policies related to emerging technologies. For example, data classification, access control, and audit logging techniques may be used in the implementation of cloud-based machine learning applications (Fallatah et al., 2024). In order to reduce human error

and resistance, policy design, training initiatives, and user interface enhancements can all benefit from an understanding of employee acceptance of such tools.

2.7.3 Diffusion of Innovation Theory

Originally developed by Everett Rogers in 1962, the DOI Theory offers a fundamental perspective for analyzing how innovations, such as emerging technology, are embraced and spread over time within a social system (Hasani et al., 2023). Fundamentally, the idea asserts that five key characteristics, relative advantage, compatibility, complexity, trialability, and observability, have an impact on an innovation's chances of being adopted. In the context of cybersecurity risk within emerging technologies, DOI provides an organized method for examining how people, companies, and sectors either adopt or reject security-oriented innovations and how these trends affect the general risk environment (Ashogbon, 2021). The DOI framework becomes especially pertinent when applied to cybersecurity in new technologies, including blockchain technology, edge AI, quantum computing, and 5G, in order to comprehend the lag between the adoption of suitable security policies and technological innovation (Faklaris, 2022). As an example, even though IoT devices are being deployed in the healthcare and industrial sectors at a rapid pace, the adoption of strong cybersecurity measures is lagging behind, which increases systemic risks.

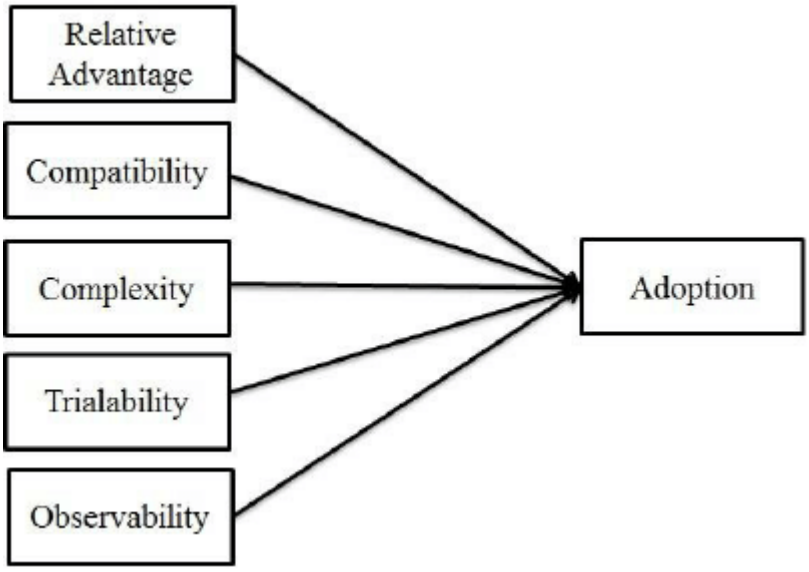


Figure 3: Characteristics of Diffusion Innovation Theory

Another important component of the DOI theory, ***"relative advantage,"*** is crucial in influencing security-related choices in contexts involving emerging technologies. Businesses are more inclined to implement cybersecurity solutions that show definite advantages over existing procedures (Hasani et al., 2023), like zero-trust architecture taking the place of conventional perimeter-based protections. However, with many new technological implementations, the advantages of some security innovations, such as homomorphic encryption in AI models, might not be immediately apparent, which prevents them from spreading (Vsevolozhsky, 2022). Through the use of DOI theory, researchers can examine how various adopter categories, including innovators, early adopters, early majority, late majority, and laggards, perceive these benefits and how they affect risk mitigation strategies.

In legacy financial or political infrastructures, ***compatibility,*** the degree to which an innovation fits in with current beliefs, processes, and practices, is especially important when implementing blockchain technology or quantum-resistant cryptography. The cybersecurity posture is undermined by high degrees of incompatibility, which frequently result in unsafe workarounds or incomplete integrations (Faklaris, 2022). For instance, incorporating blockchain technology into conventional supply chain management systems while fully comprehending the weaknesses of smart contracts may result in the creation of new, vulnerable points of failure.

The deployment of IoT ecosystems, which frequently comprise heterogeneous devices with varying firmware, communication protocols, and computational capacities, is greatly impacted by the attribute of ***complexity***. The probability of incorrect settings, unsafe defaults, and inadequate key management rises with complexity. According to DOI, adoption of technology deemed excessively complicated would be slower; nevertheless, in certain industries (Ashogbon, 2021), such as manufacturing or healthcare, regulatory requirements and external pressures may compel quick implementation irrespective of security readiness, increasing risk exposure.

Observability and trialability are also critical. Because of their hardware needs and early stage of commercialization, emerging technologies such as quantum computing present few chances for trial and proof-of-concept testing in real-world settings. Because of this, organizations frequently function in a state of uncertainty and lack empirical data regarding performance or possible weaknesses (Vsevolozhsky, 2022). Likewise, in situations where observability is restricted, like in proprietary cloud infrastructure or opaque AI decision systems, it is difficult for

enterprises to audit security postures, identify irregularities, or comprehend the consequences of system failure.

Additionally, DOI divides adopters into groups with varying risk tolerances: ***innovators, early adopters, early majority, late majority, and laggards.*** Early adopters and innovators are frequently tech-driven organizations prepared to take on greater cybersecurity risk in return for a competitive edge (Kanwal et al., 2024). On the other hand, when threat actors advance downstream, late adopters may profit from hardened systems but also face difficulties with new attack vectors. For instance, as AI becomes more commonplace, hackers start focusing on smaller businesses that don't have the same strong security systems as early adopters.

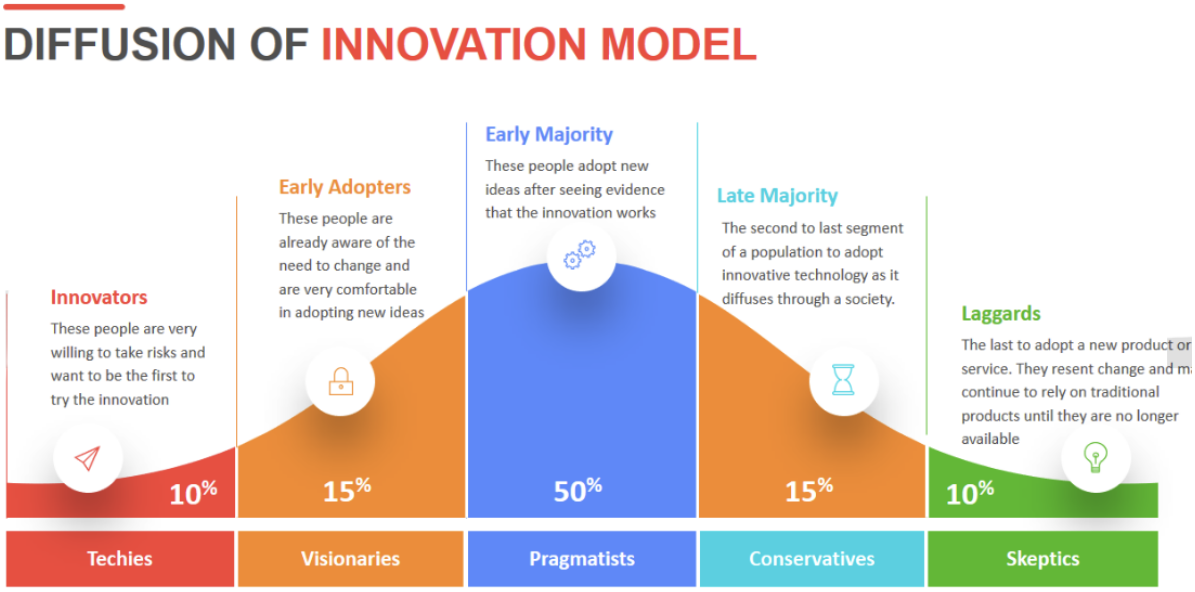


Figure 4: Adopter of DOI Theory

When these theories integrate synergistically, a more comprehensive view of cybersecurity risk mitigation regarding emerging technologies emerges. RMF offers a control-based and procedural architecture that guarantees technological and organizational management of security (Razikin & Soewito, 2022). Its efficacy is limited; nevertheless, when stakeholders or end users disregard security precautions, in this case, TAM is crucial in detecting acceptance challenges. Meanwhile, DOI describes how advancements in cybersecurity policies spread both inside and between businesses and sectors, shedding light on the factors that influence adoption, such as systemic inertia or accelerators. Despite TAM-aligned interfaces and RMF-compliant

architectures, blockchain adoption for safe supply chain management (Kure et al., 2022), for instance, may be strong at the pilot level (innovators and early adopters) but falter in mass deployment because of concerns about visibility (complexity and observability) and interoperability.

Additionally, the multilayered nature of cybersecurity risk is revealed by combining these models. While behavioral risks like phishing susceptibility or weak password practices are highlighted by TAM, technological risks like code vulnerabilities and hardware-based threats are addressed by RMF controls (Razikin, & Soewito, 2022). The structural risks associated with industry-wide adoption lags, inter-organizational dependencies, and organizational inertia are captured by DOI (Kanwal et al., 2024). In the case of 5G infrastructure deployment, for instance, even if RMF guarantees adherence to baseline standards and TAM forecasts positive user acceptance of security features, systemic risks will still exist if the diffusion of best security practices among stakeholders, including device manufacturers, telecom operators, and regulators, remains unequal.

2.8 Research Hypothesis

The following study hypotheses are put up in light of the previously mentioned discussion:

Hypothesis 01 – Classification of major cybersecurity risks has a positive influence on cybersecurity risk management in emerging technologies.

Hypothesis 02 – Technological vulnerabilities have a negative influence on cybersecurity risk management in emerging technologies.

Hypothesis 03 – Effectiven**ess** of cybersecurity frameworks has a positive influence on cybersecurity risk management in emerging technologies.

Hypothesis 04 – Targeted cyberattacks have a negative influence on cybersecurity risk management in emerging technologies.

Hypothesis 05 – Organizational, technical, and regulatory challenges have a negative influence on cybersecurity risk management in emerging technologies.

Hypothesis 06 – Governmental and industrial preparedness has a positive influence on cybersecurity risk management in emerging technologies.

3. CHAPTER 03 – RESEARCH METHODOLOGY

3.1 Research Philosophy

According to Mbanaso et al., philosophy is the primary investigation of universal and basic issues, such as those relating to the real world, knowledge, and global values (2023). The key objective of philosophy is to use a systematic, analytical strategy and its reliance on logical reasoning to find philosophical interpretations for every issue. Philosophical inquiry, which seeks to understand knowledge, truth, and universal ideals, is divided into three main schools of thought (Bergmann, 2023). A systematic, scientific examination aimed at uncovering new information is called research. The results, which are based on fundamental philosophical concepts, are applied to all research issues.

In line with Bergmann (2023), a collection of assumptions and viewpoints on the progress of knowledge is referred to as research philosophy. Even though this may seem highly advanced, a researcher is genuinely deepening their understanding of a certain subject when they begin a research endeavor. Researchers are learning new things by resolving a particular problem in a particular organization, even though their research on new knowledge growth might not be as innovative as a unique theory about human motivation. Research philosophy was categorized by Mbanaso et al. (2023) into four groups: pragmatism, positivism, interpretivism, and critical realism.

3.1.1 Pragmatism Philosophy

As its name suggests, pragmatist philosophy emphasizes the relevance and usefulness of research findings, using a more flexible and pragmatic approach than traditional all-or-nothing, mutually restricting philosophical belief systems, as described by Guo (2023). This allows the researcher to apply diverse viewpoints to a range of study variables in order to explore research aims that extend beyond philosophical boundaries.

3.1.2 Positivism Philosophy

Hoda (2024) defines positivism as the conviction that the only reliable source of knowledge is experience. According to positivism's fundamental tenet, research must be value-free, emphasize observation, and produce facts and perspectives that are consistent with an independent reality. The core technique of the scientific method is the experiment in which the practical application

of the subjects being studied overrides the prevailing belief that only issues that can be evaluated may be addressed.

3.1.3 Interpretivism Philosophy

The interpretivism concept, to comply with Sandiford & Schührer (2025), is typically the basis of studies that attempt to understand the meaning and interpretations that people assign to their experiences. An interpretivist philosophy is also frequently represented through the application of a qualitative approach that relies on methods such as interviews, observations, and textual analysis (Sandiford & Schührer, 2025). Because these researches are more diversified and unique by nature, they often look at complicated social dynamics and individual perspectives.

3.1.4 Realism Philosophy

Realism, as reported by Gamage (2025), is a viewpoint that recognizes the existence of an eventual reality while also acknowledging that individuals recognize it through their own experiences and insights. Critical realists sustain that our observation of the external world is constrained and designed by our social and cultural settings, even though it exists.

As per the researcher, the positivist research philosophy is most appropriate for this study on cybersecurity risks in emerging technologies. Positivism accentuates empirical measurement, objectivity, and hypothesis testing, aligning with the study's intention to analyze cybersecurity risk aspects, evaluate current frameworks, and examine relationships among identified variables. Positivism encourages the production of generalizable results by using quantifiable measurements and systematic data collection. This philosophical position enables the researcher to remain far from the topic, protecting objective analysis and enhancing the reliability of hypotheses based on observable facts on cybersecurity threats in developing technologies.

3.2 Research Approach

Research methodologies can incorporate a range of analytical and data gathering techniques, including surveys, experiments, case studies, observations, interviews, and archival studies, as defined by Duque et al. (2022). But according to Weiss and Johnson-Koenke (2023), a research methodology provides a thorough description of the methods and techniques the researcher intends to use for gathering, analyzing, and interpreting data. Duque et al. (2022) distinguish between three types of research approaches: abductive, deductive, and inductive.

3.2.1 Inductive Approach

ssAs defined by Diller and Passmore (2023), the inductive method focuses on creating notions or abstractions which are supported by certain patterns, evaluations, or indications in actual circumstances. With an inductive technique, researchers first collect information and observations, look for trends or patterns underlying the data, followed by use those patterns to develop sources or hypotheses. This method enables researchers to examine many points of view and provide fresh ideas or hypotheses based on the data, according to Sabharwal and Miah (2022). Observations, interviews, and content analysis are all common components of qualitative research methodologies.

3.2.2 Deductive Approach

However, as Hall et al. (2023) explain, the deductive approach begins with a fundamental idea or hypothesis and then collects and evaluates facts to confirm, validate, or disprove it. From hypothesis to facts, a systematic and organized process is followed. As stated by Manjarres & Zwierewicz (2021), the deductive method ensures a thorough and scientific procedure that grants researchers permission to approve and defend pre-existing concepts. This procedure involves formulating a hypothesis and then testing it using various assertions. In the natural sciences, laws are the most widely used research approach. They also help to explain things, make predictions about them, and eventually offer us the ability to govern them (Hall et al., 2023).

3.2.3 Abductive Approach

The abductive technique contains the underpinnings of both induction and deduction. It involves first making broad hypotheses or opinions based on documented theories, then gathering and analyzing data to improve or validate them (Hurley et al., 2021). Abduction is mainly useful when mitigating complex or unclear research problems. The abductive approach supports researchers better recognize the research problem by allowing them to direct uncertainty and take into consideration a number of reasonable explanations. Following Acero et al. (2023), an abductive approach works from back and forth, fundamentally merging induction and deduction, instead of moving from facts to theory (which take in induction) or theory to facts (which take in deduction). This is in line with the actual research of many business and management scholars, as we have already stated.

Given the quantitative nature of this study on cybersecurity risks in emerging technologies, a deductive research approach is most suitable. The deduction approach begins with established theories, such as the RMF and TAM, and formulates hypotheses that can be empirically tested through data collection and statistical analysis. This approach allows for a systematic examination of the relationships between cybersecurity threats, vulnerabilities, and mitigation strategies. By applying theory-driven hypotheses to a measurable context, the deductive method ensures that conclusions are logically derived, objective, and generalizable, aligning with the study's intent of validating theoretical constructs through empirical data.

3.3 Research Strategy

Research strategy, given by Mtisi (2022), is the broad framework or approach for conducting research. It involves choices about data collection, data processing, and the sequence of research activities. On the other hand, according to Lavarda and Bellucci (2022), the researcher's philosophy is the primary emphasis of the research plan. Although researchers are not required to voice a particular opinion, a well-thought-out plan is necessary for a scientific investigation to be properly planned and carried out. The level of investigation and the intended level of generalization dictate the researcher's approach, while the researcher's ideology generates the study aims and hypotheses (Mtisi, 2022).

Therefore, the research strategy maintains an appropriate equilibrium between the theoretical concepts discovered throughout the body of existing literature and the newly established concepts in theory that, in turn, motivate additional theoretical concerns by using real-world investigations and evaluations during the implementation of the theoretical discoveries (Lavarda & Bellucci, 2022). The process of discovery itself is supported by systems that reflect and think. In the opinion of Mottron et al. (2021), there are various types of research strategies, including quantitative, qualitative, and mixed-method strategies.

3.3.1 Quantitative Strategy

To test hypotheses, find trends, and simplify the population, the quantitative research strategy is driven by the collection and analysis of numerical data (Mottron, 2021). To ascertain the minimum requirements of variables, find connections, and arrive at trustworthy hypotheses, this approach makes use of methodical approaches, including experiments, surveys, and statistical

analysis. Pecoraro et al. (2022) claim that quantitative methods provide comprehensive and unbiased data that facilitates statistically inferring and the strength of basic correlations.

3.3.2 Qualitative Strategy

On the other hand, the qualitative strategy focuses on comprehending and expressing the meanings, events, and social circumstances of people or groups (Al Rashdan et al., 2021). These techniques compile non-numerical data using techniques including analysis of documents, interviews, and observations. According to Mottron et al. (2021), qualitative approaches produce comprehensive and in-depth data that capture the diversity and complexity of social changes and human experiences.

3.3.3 Mixed-Method Strategy

A comprehensive understanding of the study's problem is provided by the mixed-methods approach for reviewing, which combines the advantages of qualitative and quantitative approaches into a single study (Al Rashdan et al., 2021). By bringing together a variety of viewpoints, this approach enables researchers to validate results, integrate discoveries, and get deeper insights. It entails gathering and evaluating statistical and non-numerical data.

The researcher claims that a quantitative approach to research is best suited for this investigation of cybersecurity risks in emerging technologies. By using standardized tools such as surveys and exclusive questionnaires, this method enables the collection of quantitative information for statistical analysis of correlations and trends. The quantitative method makes it possible to objectively assess risk factors, vulnerabilities, and organizational actions by facilitating hypothesis testing based on theoretical frameworks like RMF and TAM. In evaluating the ways that various cybersecurity risks impact emerging technologies across sectors, this method ensures rigor, generalizability, and repeatability through the use of quantitative metrics, producing reliable, data-driven insights to inform practice and policy.

3.4 Data Collection Procedure

The practice of gathering information or proof to address the study questions is known as data collection. According to Mazhar et al. (2021), it necessitates choosing suitable methods and strategies for compiling pertinent and in-depth data. The type of phenomena under consideration, the goal of the study, and the resources at hand should all be taken into consideration while choosing data collection techniques. Throughout the data collecting phase,

researchers are responsible for maintaining the validity and reliability of the data, treating participants with respect, and correctly video capturing the data (Vogel et al., 2021).

It is acceptable because data collection delivers practical knowledge that either supports or opposes study hypotheses or objectives. Researchers can intensify the validity and reliability of their results by using different methods, including observations, interviews, surveys, experiments, and analysis of documents to acquire either first-hand or second-hand data (Mazhar et al., 2021). Ethical data collection practices ensure the accuracy and dependability of the collected data, which is essential for conducting trustworthy research.

3.4.1 Primary Source of Data Collection

From primary sources, a researcher can obtain high-quality data that can enhance the findings of their investigation. Even more data can be added as needed by researchers during the process (Daulatkar & Deore, 2022). It can be difficult to define a number of terms utilized during primary data collecting, including the kind of data collection method, the objective of data collection, exactly what should be gathered, and when to collect it. It is also an expensive approach that consumes a large portion of the study's budget and necessitates funding from many bodies (Afaq et al., 2023). The researcher can ensure the quality of the data acquired by carefully collecting data, eliminating other information, and refraining from using false or manipulated data. A range of methods, such as surveys, questionnaires, interviews, and experiments, can yield primary data (Daulatkar & Deore, 2022).

3.4.2 Secondary Source of Data Collection

In distinction, secondary sources of data collection include using previous data that has been collected by other researchers, institutions, or sources for purposes distinct from the present study effort (Shakeel et al., 2023). Orientations to secondary sources of data include scholarly journals, official publications, reports, documents, and historical documents. Secondary data is exploited by researchers to increase or assist their original research by providing background information, providing context, or comparative analysis. It makes it conceivable to analyze data that might be costly, hard, or impractical to gather directly. It can also support research design and provide a standard for comparison of primary data (Shakeel et al., 2023). However, researchers should reconsider the validity and reliability of these settings in order to get factual results.

In order to gather primary data for this study on cybersecurity threats in emerging technologies, experts actively involved in cybersecurity, IT infrastructure, and emerging technology deployment will be the target of a structured online survey questionnaire. The survey's closed-ended questions and Likert-scale items are intended to evaluate perceived vulnerabilities, the nature of risks related to cybersecurity, and the efficacy of current risk mitigation techniques. Qualtrics or Google Forms are two safe online platforms that will be used to administer the survey. This method guarantees consistent data gathering, makes it easier to quantify replies effectively, and permits thorough statistical analysis in line with the goals of the study.

3.5 Data Collection Tools

Data collection tools consist of paper surveys and computer-assisted interviews, among other equipment or devices (West et al., 2022). Observation, interviews, survey questions, and periodic examinations are a few examples of data-gathering instruments. Data collecting tools are important because research is done in many different ways and for many reasons (West et al., 2022). The goal of data collection is to get high-quality data that will allow analysis to generate reliable and convincing answers to the questions raised.

3.5.1 Observation

The process of observing and recording research participants' behavior in their natural setting is known as observation. This allows researchers to get firsthand data and learn about real-world behavior. Yujia et al. (2022) describe observation as the exact observation and documentation of events while they unfold in nature with regard to their cause, influence, or interrelationships.

3.5.2 Interviews

A face-to-face conversation between two individuals with the specific goal of gathering information relevant to the study's goals is called an interview. Interviews can be classified as irregular, significantly structured, or structured (Cheron et al., 2022). Every style differs somewhat from the others. It is expected that interviews will expand the scope of knowledge regarding the subjects being studied because they are a less organized and more naturalistic process of data collection (Cheron et al., 2022).

3.5.3 Survey

A survey questionnaire is a written or digital document that contains a collection of pre-formulated questions. These survey questions are distributed to a set of respondents, or

individuals selected for the study, who then answer them independently (Chauhan et al., 2023). The questionnaire's objective is to collect data from the group. It ought to be made strong that it is a part of the research, not the research itself. There are several procedures used in the survey data collection process (Chauhan et al., 2023).

The primary data collection tool for the current research will be a well-organized survey with response options that vary from "Strongly Aagree" through "Strongly Disgree," all based on a Likert scale of 5 points. This specific tool is designed to document experts' thoughts, experiences, and assessments on cybersecurity risks associated with emerging technologies. Sections of the survey will be clearly defined and aligned with the study's objectives. Organizational preparedness, exposure to risk, vulnerability perception, and risk mitigation strategies are some of the subjects that will be discussed in these sections. The validity and reliability of the tool for the intended audience will be ensured by the fact that each survey question is founded on tried-and-true elements from the collection of recent cybersecurity literature.

3.6 Population & Sample Size

In the setting of research, the population is referred to as an evidently defined set of objects of investigation that structure the research's focus. According to Staines et al. (2022), the initial letter N represents the number of individuals that make up the population. These units of analysis can be used to examine a group of people, countries, organizations, agencies, news reports, years, events, literature, amendments, decisions, scores, laws, etc. However, for convenience or necessity, researchers may restrict data collection to a sample of the broader population if they lack the time or resources to collect data for the entire population. Desidera et al. (2021) define a sample as any specific set of units drawn from a population. Its size is denoted by a lowercase n. The components that make up the sample are also referred to as "individuals" or "elements." Since the researcher in the present scenario could have lacked the time, resources, or accessibility to collect data from every e-commerce expert and customer worldwide, several participants (n) will be selected from the target audience (Bofill et al., 2022).

Statistical analysis is used to analyze sample-based data; sample data is used to calculate several statistics, such as the standard deviation and mean. Certain characteristics of the sample data are summarized or described by these sample statistics (Desidera et al., 2021). Researchers can

make certain conclusions by analyzing these data using other statistical methods. They used the sample statistics to estimate the population accordingly. Accordingly, the researcher uses the sample mean and the population average standard deviation, given the sample standard deviation, to calculate the population mean (Staines et al., 2022).

The target population for this research comprises cybersecurity professionals, IT managers, system administrators, and technology analysts actively involved in managing or overseeing cybersecurity operations within organizations that utilize emerging technologies. These individuals are selected due to their direct exposure to and experience with the cybersecurity risks, threat landscapes, and mitigation strategies relevant to rapidly evolving technological ecosystems. Given the study's aim to gather statistically relevant insights, a sample size of 200 respondents has been determined. This sample size is appropriate for achieving sufficient statistical power and reliability in analysis, which will be analyzed through descriptive and inferential statistical methods.

3.7 Sampling Technique

The process and strategies used to pick a particular subset of units across a population, in our example, selecting e-commerce professionals, are referred to as research sampling approaches (Van Haute, 2021). When compared to working with the entire population, sampling procedures have a detrimental effect on accuracy and comprehensiveness, although they save money on data gathering costs. Biases or errors may exist in the gathered data. According to Golzar et al. (2022), the two main decisions that affect the extent of the margin of error and the accuracy with which the results of sample research can be extrapolated to the entire population are the study technique and sample size. Researchers use probability sampling and non-probability sampling as their two main techniques for sampling. The probability of a participant or element being included in the sample can be indicated by a researcher using probability sampling. It is hard to predict whether an element will be included in a sample when non-probability sampling is used (Ahmed, 2024).

3.7.1 Probability Sampling

Probability sampling, following Rahman et al. (2022), refers to sampling practices in which each member of the total population has an equivalent opportunity of being nominated for the sample. By providing each variable within the group of participants an equal opportunity of being

selected, this technique ensures an impartial representation of the total population. Among the techniques used in probability sampling are elementary random sampling, stratified sampling, cluster sampling, and systematic sampling (Van Haute, 2021). Probability sampling has the advantage of enabling researchers to pinpoint specific bias and inaccuracy in relation to the data collected. Four types of probability sampling are identified by Sarker and Al-Muaalemi (2022): stratified random sampling, cluster sampling, random sampling, and systematic random sampling.

3.7.2 Non-Probability Sampling

Non-probability sampling has the advantage of being a practical way for researchers to create a sample at no or minimal cost for studies that do not require population representativeness (Adeoye, 2023). Non-probability sampling is a helpful method to use when conducting a pilot study, attempting to interview groups that could potentially be susceptible to the questions and not want to answer them honestly, or in situations where ethical considerations prohibit the researcher compared to interviewing each member of a particular group (Ahmed, 2024). Non-probability sampling can be further classified into four categories, according to Futane & Tech (2021): quota, convenience, purposive, and snowball sampling.

For this study on cybersecurity risks in emerging technologies, a probability sampling technique, specifically stratified random sampling, is deemed most suitable. Stratified random sampling empowers the researcher to divide the target population into distinct subgroups or strata based on relevant characteristics such as industry sector (e.g., finance, healthcare, government, manufacturing) or organizational role. This approach ensures that each subgroup is proportionately represented in the final sample, enhancing the representativeness and generalizability of the findings. Every person in each stratum has an equal chance of being chosen when stratified random sampling is used, which reduces the potential biases resulting from non-probability techniques.

3.8 Description of Participants of the Study

The study's participants will mostly be cybersecurity experts who are actively involved in mitigating the risks posed by developing technology. This group will include of technology compliance officers, risk assessment experts, system administrators, cybersecurity analysts, and IT security managers from a variety of industries, including government, telecommunications,

healthcare, and finance. To guarantee knowledgeable and pertinent answers, participants must have worked directly on cybersecurity challenges pertaining to cutting-edge technologies, including cloud computing, blockchain, IoT, and AI for at least two years.

In order to gather a wide variety of viewpoints on cybersecurity risk management, the sample will comprise people from businesses of various kinds, ranging from small and medium-sized businesses to multinational firms, and from both developed and emerging digital economies. In order to reflect the diversity of professionals in the cybersecurity field, demographic variables like age, gender, and educational background will also be taken into account. Participants will be found and recruited through industry-specific forums, cybersecurity conferences, professional networks, and LinkedIn groups focused on cybersecurity and new technologies. The recruiting strategy aims to ensure a proportionate cross-sectional of individuals who deal with different types of cyberattacks and organizational challenges. This will facilitate a better understanding of risk viewpoints, vulnerabilities, and mitigation strategies as a whole.

Every step of the data collection process will adhere strictly to ethical standards, which include confidentiality, informed consent, and voluntary involvement. The quantitative information obtained from the respondents selection procedure will certainly be reliable, valid, and relevant to the greater community of cybersecurity experts addressing emerging technological issues.

3.9 Research Tool & Development

A standardized survey questionnaire was created especially for cybersecurity experts and technology managers who manage new technologies in order to guarantee agreement with the study's goals. In accordance with the approach developed by Likert (1932), the questionnaire consisted of 30 items that were scored on a 5-point Likert scale, with 1 denoting "strongly disagree" and 5 denoting "strongly agree" (Malik et al., 2021). Following Schrum et al. (2023), this scale was used to measure respondents' perceptions of cybersecurity vulnerabilities, risks, and mitigation techniques in developing technologies without supposing equal time between points. The efficacy of cybersecurity frameworks, organizational obstacles, risk identification, and vulnerability assessment were among the important topics covered in the questionnaire. Prior to distribution, the tool was validated by experts and tested in a pilot research to ensure its clarity, relevance, and reliability. This ensured that the tool would produce accurate and

quantifiable data that could be used for statistical analysis and testing of hypotheses in the quantitative study.

The questionnaire's main components are statements that gauge believed cybersecurity risks, vulnerability awareness, and the implementation of mitigation strategies. To gauge the degree of agreement or concern, responses are scored on a 5-point Likert scale that goes from "strongly disagree" to "strongly agree." The primary research instrument used in this study to assess cybersecurity risk viewpoints, vulnerabilities, and mitigation strategies in emerging technologies is a structured quantitative questionnaire. The questionnaire was developed after a careful examination of risk management models, existing cybersecurity frameworks, and recent empirical studies on security issues. It aims to collect detailed perspectives from cybersecurity professionals on the frequency of various cyberthreats, the effectiveness of existing risk management practices, and organizational preparation.

The tool also has items that assess organizational concerns, regulatory compliance, and the perceived appropriateness of cybersecurity frameworks that are updated to reflect changing technological trends. A few examples of statements that provide insight into regulatory alignment and institutional readiness are "Our policies regarding cybersecurity are often revised to reflect new risks within emerging technologies," and "adherence with international requirements for cybersecurity has been successfully integrated into our risk prevention actions." To successfully gather data and reach a wide number of geographically scattered cybersecurity professionals, the questionnaire is sent electronically using Google Forms. This research technique may be used to statistically examine cybersecurity risk factors in evolving technology contexts, producing credible and trustworthy data that help the study achieve its objectives.

3.10 Data Analysis

Data analysis is defined as the process of classifying, evaluating, and interpreting the collected data. According to Dey and Wang (2022), it is the procedure of changing formless data into meaningful inferences. Data analysis can use different techniques, such as theme analysis, content analysis, statistical analysis, and narrative analysis. In the opinion of Salmona and Kaczynski (2024), the research queries, the kind of data collected, and the procedure used all impact the specific technique selected. The objective of data analysis is to recognize patterns, relationships, and trends in the data in order to reach at decisions or inferences that support the

research's objectives. Researchers can guarantee the validity and precision of their findings by using the suitable analytical tools, procedures, and techniques (Dey & Wang, 2022).

3.10.1 Thematic Analysis

Thematic analysis is identified as a more complex form of analysis that includes many steps, such as familiarization (understanding and transcription of the data), the formation of a thematic framework (the initial coding outline that is developed both before and after experiencing problems) (De Fina, 2021), coding (through the utilization of textual or mathematical codes to recognize actual information points that interpret to different themes), charting (by put on headings employing the thematic framework to produce charts), mapping, and decoding (reflecting for relations, concepts, and patterns, explanations in the collected data) (Alzubaidi et al., 2023).

3.10.2 Content Analysis

The process of sensibly reading and analyzing written, spoken, or visual information to classify specific themes, patterns, or characteristics is identified as content analysis (Alzubaidi et al., 2023). By gauging and categorizing the material of the data, researchers can employ this method to find acquaintances, patterns, or trends in the manuscript. To systematically examine and categorize the content of the data, content analysis applies a structured approach that often involves coding systems or pre-defined categories.

3.10.3 Statistical Analysis

Statistical analysis is the grouping of mathematical techniques or processes for gathering, describing, categorizing, and evaluating numerical data (Bragazzi et al., 2023). Since statistics often generates such quantitative data, it is a crucial tool for measurement and research. The fundamental objectives of analysis serve as the foundation for statistical approaches, which means that the researcher using statistics is not only concerned with manipulating data (Meeker et al., 2021). Research in education may concentrate on two types of statistical analysis applications: inferential statistical analysis and descriptive statistical analysis.

3.10.4 Narrative Analysis

Narrative analysis is the process of rephrasing stories provided by respondents while accounting for the unique circumstances of each case and the diverse experiences of each respondent (Salmona & Kaczynski, 2024). In other words, researchers use narrative analysis to make

revisions to primary qualitative data. experiences that are based on narrative transcriptions. There is a narrative element to each observation or interview that the researcher must filter through, evaluate, refine, and then present to the reader within an updated version (De Fina, 2021).

The collected quantitative data will be analyzed using IBM SPSS Statistics software to provide a precise and comprehensive understanding of cybersecurity risks in emerging technologies. Initially, data cleaning and screening will be performed to check for missing values, outliers, and normality assumptions. Descriptive statistics, including means, standard deviations, and frequencies, will summarize the demographic data and key variables. For hypothesis testing, multiple statistical tests will be employed. Correlation analysis will assess the strength and direction of relationships between variables such as vulnerabilities and risk mitigation strategies. Regression analysis will be conducted to examine the predictive power of independent variables on cybersecurity risk outcomes, with the Model Summary indicating the variance explained, ANOVA testing overall model significance, and Coefficients identifying individual predictor effects. These SPSS procedures will enable robust statistical inference, ensuring valid, reliable findings that inform effective cybersecurity risk management practices in emerging technologies.

3.11 Ethical Considerations

The term ethics in research refers to the norms and guidelines that guide decisions about data gathering, analysis, and publication. Since ethical knowledge typically entails a latent character, as Kaddoura, & Al Husseiny (2023) point out, an increasing number of studies are examining the moral quandaries brought up by study evaluation. Ethics may also be defined as a method, approach, or perspective for determining one's own conduct and for interpreting complex circumstances and conundrums (Dave, 2023). For instance, one could take an ethical, political, and sustainable, or economic perspective while considering a complex issue like global warming.

In research and even in business, ethics have important considerations. For example, because of well-known companies like Enron and WorldCom, politicians, industry experts, and academic institutions have taken notice of ethical issues in business (Kaddoura, & Al Husseiny 2023). Indeed, recent reports of abuses of academic integrity have surfaced. Consequently, it is essential for researchers to understand the foundations of ethical research and how they could affect their efforts. According to Dave, (2023), research ethics encompasses more than just

filling out paperwork. It also includes performing research in a way that doesn't harm anyone, and how one communicates findings, and how one views the data, which provides ideas (i.e., precisely represents the literature). The researcher must adhere to the following ethical guidelines when carrying out this investigation.

3.11.1 Informed Consent

Researchers must get the freely informed consent of each participant prior to the start of any data collection session (Hasan, 2021). A letter of informed consent must be given to every participant. The consent letter must outline the study's main objectives and purpose, in addition to its ethical considerations, including issues with anonymity and confidentiality. Researchers must also get participants' participation and assent and stress the terms of the participant-researcher contract before starting data collection (Hasan, 2021). Furthermore, we should always ensure that our research is free of dishonesty. Deception is the deliberate utilization of research for purposes other than those initially negotiated with participants.

3.11.2 Anonymity & Confidentiality

In keeping with Kiani et al., (2022), researchers should take every precaution to protect the confidentiality of study participants and data privacy. Before data collection sessions begin, participants should be informed of these two factors and their inclusion in the researcher-participant agreement. All data must be handled and maintained in accordance with data protection legislation. Only the investigator and, if applicable, the other members of the study team should have access to the data (Kiani et al., 2022). Every document and audio recording should be stored in a secure location that is nonetheless easily reachable.

3.11.3 Updating Participants

Respondents should, whenever possible, be updated on the research's progress. A copy of the transcript, questionnaire, or responses should be provided to each participant by the researchers after the data collection is complete. A summary of the analysis performed on the collected data should also be provided to the research participants in order to prevent any misunderstandings or fabrications of the results. Wang et al., (2023) states that it is advantageous for researchers to ask participants for feedback at the end of the study and to provide them with electronic copies of the results or other publications that came from their involvement. To make any necessary

adjustments, it is essential to get participant input at any stage of the research process, as recommended by Wang et al., (2023).

3.11.4 Respect-Based Ethics

All of our study participants, especially the volunteers, need to be treated with the utmost respect and trust. The respect of participants needs to be considered in any research, regardless of their gender, age, ethnic background, religion, lifestyle, political opinions, or any other significant difference between them and the researchers themselves (Chervenak & McCullough, 2021). Each participant must thus be given equal treatment, and throughout the study, their arguments need to be thoughtfully taken into account. Respect for all participants in or impacted by the study should be the guiding principle of researchers' ethics, claim Chervenak & McCullough (2021).

4. CHAPTER 04 – RESULTS & FINDINGS

4.1 Respondent Demographics

The demographics of the respondents offer important context for understanding the findings of this quantitative research on cybersecurity risk in emerging technologies. Participants included experts from the fields of cybersecurity, information security, IT infrastructure, and technology governance, and they characterised a broad range of industries actively implementing emerging technologies. These professionals were selected because of their relevant understanding of modern cybersecurity risk management approaches and their practical experience. The sample consisted of people from the public and private sectors, on behalf of a variety of organizational types. The respondents held current roles as digital risk consultants, information systems officers, network security engineers, cybersecurity analysts, and IT managers, among others.

4.1.1 Age

Table 4: Age Distribution of Participants

Age Group	Frequency	Percentage (%)
18 to 24 years old	48	**24.00**
25 to 34 years old	62	**31.00**
35 to 44 years old	45	**22.50**
45 to 54 years old	28	**14.00**
55 and above	17	**8.50**
Total	**200**	**100**

The age distribution of the respondents included for this study reflects a broad sample of professionals engaged in cybersecurity-related initiatives across organizations using emerging technology. According to Table 4, the highest percentage of participants (31 percent), or 62 people, are between the ages of 25 and 34. Professionals in their early to mid-career stages are usually represented in this cohort, and many of them are actively involved in the organizational and implementation levels of cybersecurity procedures. Their inclusion offers critical insights into hands-on challenges and practical exposure to technological vulnerabilities within emerging digital ecosystems.

The second most represented group is the 18 to 24 years old bracket (24 percent, or 48 participants), suggesting a notable engagement of younger professionals, interns, or recent graduates, particularly those entering the cybersecurity workforce. Their viewpoints are important for documenting changes in academic readiness, digital literacy, and understanding of current cyberthreats. 45 responders (22.5 percent), who are between the ages of 35 and 44, are probably mid- to senior-level professionals having strategic responsibilities, such as governance and risk management positions. Their views contribute to understanding how cybersecurity risks are mitigated from a managerial and policy implementation standpoint.

Experienced professionals who may have an impact on infrastructure choices, organizational security frameworks, and policy formation are included in the 28 participants (14 percent) in the 45–54 age group. Their observations are particularly helpful in assessing cybersecurity's long-term resilience and ability to adjust to swift technical advancements. Finally, 17 responders (8.5 percent) are above 55 and represent senior leadership or very experienced professionals. Despite having fewer members, this organization provides historical and strategic insights into enterprise-level cyber protection procedures, risk evolution, and compliance.

4.1.2 Gender

Table 5: Gender Distribution of Participants

Gender	Frequency	Percentage (%)
Male	104	**52.00**
Female	89	**44.50**
Prefer not to say	07	**3.50**
Total	**200**	**100**

The gender distribution of participants in this quantitative study, which examines cybersecurity risk management in relation to new technologies including cloud computing, blockchain, IoT, and AI, is shown in Table 5. The bulk of the sample, 104 individuals (52 percent), identified as male, according to the statistics. This representation is consistent with larger industry trends, which show that more men are working in information technology and cybersecurity. The

viewpoints of this group are crucial to understanding the attitudes and practices that are common in the traditionally male-dominated technology sector.

A significant number of respondents, 89, or 44.5 percent, identified as female. This significant female involvement indicates that there is an increasing gender diversity in cybersecurity and emerging IT professions. Their participation improves the study by including a greater range of professional perspectives and experiences, particularly about risk assessment, policy enforcement, and secure system design. Incorporating female viewpoints into cybersecurity research is especially crucial since it increases the findings' inclusion and generalizability. The choice "Prefer not to say," which was chosen by seven respondents (3.5 percent), also suggests a notable trend in professional surveys in the direction of preferences for privacy and self-identification. While recognizing the evolving standards in gender reporting, this inclusion advances the ethical ideals of voluntary transparency and anonymity in research.

4.1.3 Highest Educational Qualification

Table 6: Highest Educational Qualification of Participants

Educational Qualification	Frequency	Percentage (%)
Professional Certification (e.g., CEH, CISA, CISSP)	28	**14.00**
Bachelor's Degree	72	**36.00**
Master's Degree	65	**32.50**
Doctorate (Ph.D.)	21	**10.50**
Other (please specify)	14	**7.00**
Total	**200**	**100**

A detailed examination of the highest educational levels attained by the participants in this quantitative study is provided in Table 6, with a focus on cybersecurity risk in emerging technologies. Since it demonstrates the level of knowledge and theoretical underpinning that defines their viewpoints and professional actions, the participants' diverse educational backgrounds have a crucial role in influencing the validity and scope of the insights gained. The largest group of participants, 72, or 36 percent of the total, have a bachelor's degree. This demonstrates their solid background in relevant subjects, most likely information technology,

computer science, or related fields, which equips them with the fundamental understanding required to address cybersecurity challenges in quickly evolving technological environments. The second-highest place is held by 65 responders (32.5 percent) who have a master's degree, suggesting a high academic expertise.

Meanwhile, data show that 28 people, or 14 percent of the sample, hold professional certifications such as CISA (Certified Information Systems Auditor), CEH (Certified Ethical Hacker), and CISSP (Certified Information Systems Security Professional). These qualifications, which demonstrate particular industry-recognized expertise, emphasize practical skills and adherence to professional standards in cybersecurity risk management. Their input is crucial for assessing the practical implementation of security regulations and mitigation techniques in emerging technology. Additionally, 21 responders (10.5 percent) have a doctorate (Ph.D.), the highest academic level. This subgroup most likely consists of academics and senior cybersecurity experts who have a thorough knowledge of theoretical frameworks, statistical techniques, and state-of-the-art cybersecurity technology. Their insights are particularly useful for navigating strategic actions and understanding complex risk concerns in quickly evolving technological domains. Finally, "Other" qualifications, which may include associate degrees, certificates, or interdisciplinary educational backgrounds, were chosen by 14 participants (7 percent).

4.1.4 Current Role / Job Title

Table 7: Current Role / Job Title of Participants

Roles	Frequency	Percentage (%)
IT Manager	42	**21.00**
Cybersecurity Analyst	38	**19.00**
Information Security Officer	33	**16.50**
Risk Officer	29	**14.50**
Security Engineer	27	**13.50**
Network Administrator	21	**10.50**
Other (please specify)	10	**5.00**
Total	**200**	**100**

Table 7 presents a comprehensive summary of the professional roles that the participants in the current study on cybersecurity concerns in emerging technologies hold. The range of occupations included provides crucial context for understanding the organizational perspectives and real-world experience that inform the research findings. Of the total replies, 42 people (or 21 percent) were identified as IT managers. These professionals are often in charge of planning, directing, and executing IT infrastructure and security protocols inside companies. In emerging technology settings like as AI, IoT, and cloud computing, their role often involves strategic decision-making related to cybersecurity risk management in order to offer a holistic organizational view.

Following that, 38 individuals (19 percent) revealed that they were cybersecurity analysts. These individuals focus on identifying, assessing, and mitigating security threats and vulnerabilities. Their expertise is crucial for assessing emerging risks and the effectiveness of cybersecurity defenses, particularly in environments vulnerable to sophisticated attacks. According to 33 participants (16.5 percent), information security professionals are essential to the development and execution of security protocols and compliance measures. Their function ensures corporate compliance with regulatory requirements and increases resistance against vulnerabilities found in emerging technology. Recognizing and managing organizational risks, including cybersecurity hazards, is a specialty of risk officers. They comprise 14.5 percent, or 29 responders. Their risk-based methodology is essential for evaluating the consequences of technological errors and the applicability of mitigation strategies employed in quickly evolving tech settings.

Security engineers, with 27 members (13.5 percent), are responsible for the design, installation, and upkeep of secure networks and systems. Their technical expertise directly affects the strength of defenses regarding cyberattacks that target emerging technologies; therefore, understanding the effectiveness of practical mitigation requires their judgments. Network administrators, who comprised the 21 participants, or 10.5 percent of the sample, are responsible for monitoring and maintaining the security of the network infrastructure. Their operational role sheds light on the everyday and technical challenges of defending networks against emerging cyberthreats. Finally, ten participants (5 percent) identified as Other, indicating other positions

like IT auditors, compliance officers, or specialist consultants. This subgroup adds even more variety by adding a range of viewpoints on cybersecurity risk management to the data.

4.1.5 Years of Experience in IT / Cybersecurity

Table 8: Respondents' Years of Experience in IT / Cybersecurity

Working Years	Frequency	Percentage (%)
Less than 2 years	26	**13.00**
2 to 5 years	58	**29.00**
6 to 10 years	61	**30.50**
11 to 15 years	35	**17.50**
More than 15 years	20	**1.00**
Total	**200**	**100**

The respondents' distribution according to the number of years they have worked in the fields of cybersecurity and information technology is shown in Table 8. This demographic factor is essential for evaluating the range of competence included in the research and for comprehending how different degrees of exposure to technology settings affect how people perceive cybersecurity dangers and react to new threats. Professionals with six to ten years of experience make up the largest category, with 61 respondents (30.5 percent). People in this category usually work in mid-level or higher technical roles and have accumulated a great deal of experience with both contemporary security frameworks and ancient systems. Their views have likely been informed by their real-world experience implementing enterprise-wide cybersecurity policies, coordinating cloud service migrations, and integrating threat detection technology. They are well-positioned to evaluate both known and emerging risk reduction measures due to their tenure.

According to the 58 respondents (29 percent), those with 2 to 5 years of experience rank second. Most of this category consists of early-career professionals who may have joined the workforce during the rapid expansion of cloud-based infrastructure and digital transformation. They are often exposed to rapidly expanding environments and gain practical experience with contemporary automation systems and cybersecurity solutions. Respondents in this sector offer valuable insights on contemporary topics such as safeguarding DevOps pipelines, managing software manufacturing risks, and putting zero trust concepts into practice in hybrid cloud

settings. Of the participants, 26 (13 percent) had less than 2 years of expertise, which is typical of entry-level workers or recent graduates entering the cybersecurity industry. Their perspectives align with current onboarding practices and academic preparation for cybersecurity roles. This group is particularly relevant for understanding the gap between theoretical frameworks and their implementation in high-stakes organizational settings.

As a sign of high seniority and likely holding managerial, consulting, or strategic positions, 35 respondents, or 17.5 percent), reported having 11 to 15 years of experience. This group provides perspectives shaped by leadership in risk management, incident response planning, and regulatory compliance, particularly in large or regulated companies. Finally, 20 people (10 percent) have over 15 years of experience. These individuals are regarded as seasoned experts with a wealth of institutional experience who are able to contextualize today's cybersecurity problems within a broader infrastructural and historical framework. Their viewpoints contribute significantly to the study of long-term risk trends, organizational maturity models, and the evolution of cybersecurity culture in response to technological breakthroughs.

4.1.6 Company's Primary Technology Focus

Table 9: Respondents' Firm's Primary Technology Focus

Organization's Technology Focus	Frequency	Percentage (%)
Artificial Intelligence (AI) / Machine Learning (ML)	64	**32.00**
Internet of Things (IoT)	52	**26.00**
Blockchain Technology	34	**17.00**
5Gnetworks	21	**10.50**
Cloud Computing	70	**35.50**
Quantum Computing	13	**6.50**
Other (please specify)	16	**8.00**
Total	**200**	**100**

Table 9 displays the distribution of respondents by the primary technological domain in which their organizations specialize. The technical concentration of an organization directly affects the risks related to cybersecurity that it encounters, the risk mitigation strategies it employs, and its overall risk posture, thus, understanding this distribution is crucial. The findings provide important insight into the circumstances in which risk management for cybersecurity is used across various emerging technologies. The most often reported technological emphasis area was cloud computing, as 70 participants (35.5 percent) stated that their firms primarily operate in this area. This is consistent with the global trend of using cloud infrastructure for storage, application hosting, and business continuity. Cloud environments can, however, present additional cybersecurity risks, including the possibility of data loss, service interruptions, incorrectly set up cloud instances, and unauthorized access. A thorough examination of how these organizations handle risks associated with multi-tenancy, insecure APIs, identity federation, and adherence to changing cloud security standards like ISO/IEC 27017 and the Cloud Controls Matrix (CCM) is made achievable by the study's recognition of cloud-focused organizations.

The majority of respondents (64 people, or 32 percent) stated that machine learning and artificial intelligence are at the heart of their organization's technology operations. These businesses frequently use AI/ML for automation, predictive analytics, and decision-making. These technologies provide new types of cybersecurity threats, including algorithmic bias exploitation, data poisoning, and adversarial machine learning. These risk factors are increased by the fact that many AI models are "black boxes," making it more difficult to identify and fix problems. Examining how well-suited the present cybersecurity frameworks are to safeguarding AI-driven infrastructures is made possible by the information obtained from these respondents. 52 respondents, or 26 percent of the sample, said that the IoT is the main emphasis of their companies. IoT ecosystems are known to be highly susceptible to cyber threats due to their decentralized architecture, limited computational resources, and often inadequate security mechanisms. Devices in such ecosystems, ranging from industrial sensors to smart appliances, are often deployed with default credentials, lack encryption, and operate on outdated firmware, making them ideal targets for exploitation. The presence of IoT-focused firms in the sample provides critical data on real-world exposure to threats like botnet recruitment (e.g., Mirai), device hijacking, and lateral movement across interconnected systems.

Blockchain Technology was identified as the primary technological focus by 34 respondents (17 percent). While blockchain is inherently designed to be secure through decentralized ledger mechanisms, vulnerabilities exist in the form of smart contract bugs, private key theft, 51 percent attacks, and inadequate governance models. Respondents working with blockchain systems offer insights into how organizations are implementing cybersecurity policies to address these nuanced and often overlooked vulnerabilities, particularly within financial, healthcare, and supply chain use cases. 5G networks were reported as the main operational area by 21 respondents (10.5 percent). The rollout of 5G technology introduces new cybersecurity challenges due to its reliance on software-defined networking (SDN), edge computing integration, and massively increased connectivity. This creates a wider attack surface and introduces potential for sophisticated threats, including network slicing attacks, signalling storms, and APTs at the edge. These respondents' experiences serve as an example of how security designs are changing to support situations with high speeds and low latency.

13 respondents, or 6.5 percent of the total, indicated that quantum computing was the technological area of their company. While still in its infancy, quantum computing presents a danger to traditional encryption techniques, especially RSA and ECC, which form the basis of today's cybersecurity framework. Businesses engaged in quantum research are leading the way in creating quantum-resilient encryption and providing insights into proactive risk evaluation and solutions for future-proofing. Lastly, 16 out of the participants (8 percent) chose "other" as the technology priority for their company. These covered fields like edge computing, AR/VR, and robotics. Every one of these areas has different cybersecurity problems. For instance, edge computing presents problems with data governance and dispersed threat detection, while AR/VR may include privacy concerns with biometric data.

4.2 Descriptive Statistics

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
CLASSIFICATION OF MAJOR CYBERSECURITY RISKS	100	1.00	5.00	3.0833	.99310

TECHNOLOGICAL VULNERABILITIES	100	1.00	5.00	3.0300	.78295
EFFECTIVENESS OF CYBERSECURITY FRAMEWORKS	100	1.00	5.00	3.1567	.99770
TARGETED CYBERATTACKS	100	1.00	5.00	3.0300	.78295
ORGANIZATIONAL, TECHNICAL & REGULATORY CHALLENGES	100	1.00	5.00	3.6700	.94933
GOVERNMENTAL & INDUSTRIAL PREPAREDNESS	100	1.00	5.00	3.6667	.90267
CYBERSECURITY RISK MANAGEMENT	100	1.00	5.00	3.7067	.87909
Valid N (listwise)	100				

The descriptive statistics presented in the table above for the hypothesis "Classification of Major Cybersecurity Risks" indicate a mean value of 3.0833 with a standard deviation of 0.99310. This suggests that, on average, participants moderately agree with the relevance or significance of major cybersecurity risk classifications within emerging technologies. The relatively high standard deviation implies considerable variability in responses, reflecting differences in understanding or experience with the categorization of risks such as data breaches, insider threats, and system intrusions. The minimum and maximum scores, which span the full Likert scale range from 1.00 to 5.00, confirm that perceptions ranged from strong disagreement to strong agreement, indicating diverse viewpoints among participants.

In the case of "Technological Vulnerabilities," the mean score is slightly lower at 3.0300, with a standard deviation of 0.78295. This lower standard deviation suggests a more consistent set of

responses compared to the previous construct. The mean value, being close to the midpoint of the scale, indicates a neutral to slightly positive perception of the presence of technological vulnerabilities in systems like IoT devices, AI algorithms, or cloud infrastructures. The full range of scores again suggests that while most respondents recognize some level of vulnerability, the extent of concern varies across the sample, possibly influenced by different technical backgrounds or exposure to real-world security incidents.

For the hypothesis "Effectiveness of Cybersecurity Frameworks," the mean is recorded at 3.1567, indicating that participants lean slightly toward agreement that existing frameworks are at least somewhat effective in addressing cybersecurity challenges in emerging technology domains. However, the standard deviation is relatively high at 0.99770, pointing to a wide range of opinions. This dispersion might stem from differing levels of implementation or familiarity with frameworks such as NIST, ISO/IEC 27001, or local regulatory guidelines across sectors or regions. The broad range of responses may also reflect differing confidence levels in how well these frameworks adapt to evolving threats and rapid technological advancements.

Remarkably, the hypothesis "Targeted Cyberattacks" shows an identical statistical profile to that of technological vulnerabilities, with a mean of 3.0300 and a standard deviation of 0.78295. This suggests a similarly moderate level of concern regarding threats like spear phishing, ransomware, and zero-day exploits. The consistency in these values may point to a perceived link between technical flaws and the likelihood of targeted attacks, implying that respondents view these risks as intertwined. The consistent use of the full Likert range underscores the presence of both alarm and complacency within the respondent group.

The hypothesis related to "Organizational, Technical & Regulatory Challenges" reveals a notably higher mean value of 3.6700, suggesting stronger agreement among participants that these challenges are significant obstacles to effective cybersecurity in emerging technologies. The standard deviation of 0.94933 indicates moderate to high variability, likely due to differing organizational maturity levels, technical infrastructure, or regulatory environments among respondents. The higher average indicates that participants acknowledge that complicated internal and external obstacles, like a lack of qualified staff, a lack of funding, or disjointed policy frameworks, are important elements escalating cybersecurity threats.

With a mean of 3.6667 and a standard deviation of 0.90267, the "Governmental & Industrial Preparedness" concept exhibits a similarly high perception. This suggests that respondents typically believe that both industry and governmental entities are only somewhat equipped to handle cybersecurity risks. The variety of answers, however, indicates that although some people believe there are successful programs and partnerships in place, others believe there is a lag in readiness, which might be brought on by differences in jurisdiction, unequal investment in cybersecurity infrastructure, or inefficient public-private partnerships.

The hypothesis titled "Cybersecurity Risk Management" had the highest mean in the sample, measuring 3.7067, having a standard deviation of 0.87909. This result indicates that participants hold a slightly more favourable view of the presence and application of risk management practices, such as risk assessments, threat modelling, incident response planning, and continuous monitoring. The relatively lower standard deviation compared to other high-mean constructs suggests a more cohesive understanding or experience with risk management strategies across the sample. This may indicate that while challenges exist in other areas, structured risk management is becoming a well-established component of cybersecurity practices in organizations dealing with emerging technologies.

Correlations

		CLASSIFICATION OF MAJOR CYBERSECURITY RISKS	TECHNOLOGICAL VULNERABILITIES	EFFECTIVENESS OF CYBERSECURITY FRAMEWORKS	TARGETED CYBERATTACKS	ORG IC TEC REG CHA
CLASSIFICATION OF MAJOR CYBERSECURITY RISKS	Pearson Correlation	1	.379**	.660**	.379**	
	Sig. (2-tailed)		.000	.000	.000	
	N	100	100	100	100	
TECHNOLOGICAL VULNERABILITIES	Pearson Correlation	.379**	1	.241*	1.000**	
	Sig. (2-tailed)	.000		.016	.000	
	N	100	100	100	100	
EFFECTIVENESS OF CYBERSECURITY FRAMEWORKS	Pearson Correlation	.660**	.241*	1	.241*	
	Sig. (2-tailed)	.000	.016		.016	
	N	100	100	100	100	
TARGETED CYBERATTACKS	Pearson Correlation	.379**	1.000**	.241*	1	
	Sig. (2-tailed)	.000	.000	.016		
	N	100	100	100	100	
ORGANIZATIONAL, TECHNICAL & REGULATORY	Pearson Correlation	.256*	.279**	.408**	.279**	
	Sig. (2-tailed)	.010	.005	.000	.005	
	N	100	100	100	100	

The correlation analysis conducted in this study provides critical insights into the relationships among the key dimensions of cybersecurity risk in emerging technologies. Pearson correlation coefficients were calculated to assess the strength and direction of linear relationships between pairs of variables. A statistical significance is reported at both the 0.01 and 0.05 levels (2-tailed), allowing for a robust interpretation of inter-variable dependencies.

The variable "Classification of Major Cybersecurity Risks" demonstrates statistically significant positive correlations with all other constructs in the matrix. Most notably, it exhibits a strong correlation with "Effectiveness of Cybersecurity Frameworks" ($r = .660$, $p < .01$), indicating that respondents who recognize and understand the classification of major risks are also more likely to perceive cybersecurity frameworks as effective. This strong association suggests a conceptual linkage where accurate identification and categorization of cybersecurity risks enhance the applicability and trust in formal security models and standards. Moderate yet significant correlations are observed with "Technological Vulnerabilities" and "Targeted Cyberattacks" ($r = .379$, $p < .01$ for both), suggesting that an increased awareness of categorized risks is associated with a heightened recognition of both vulnerabilities and direct attack vectors. Additionally, weaker yet statistically significant correlations are seen with "Organizational, Technical & Regulatory Challenges" ($r = .256$, $p < .05$), "Governmental & Industrial Preparedness" ($r = .228$, $p < .05$), and "Cybersecurity Risk Management" ($r = .219$, $p < .05$). These findings indicate that although there is alignment, the influence of risk classification on broader strategic or regulatory domains may be more modest.

"Technological Vulnerabilities" is perfectly correlated with "Targeted Cyberattacks" ($r = 1.000$, $p < .01$), a rare and precise alignment that likely reflects a duplication or construct overlap in the survey items used for these two variables. This result signifies that the recognition of vulnerabilities is inseparably linked to the awareness of targeted attacks, reinforcing the notion that technical flaws often serve as primary enablers for malicious activities. In addition, technological vulnerabilities are moderately correlated with "Governmental & Industrial Preparedness" ($r = .357$, $p < .01$) and "Cybersecurity Risk Management" ($r = .355$, $p < .01$), indicating that as awareness of technical gaps increases, so does the emphasis on readiness and structured mitigation efforts. The correlation with "Effectiveness of Cybersecurity Frameworks" is slightly weaker ($r = .241$, $p < .05$), suggesting that perceived technical shortcomings are moderately linked to perceptions about the adequacy of existing frameworks. Furthermore, a moderate correlation with

“Organizational, Technical & Regulatory Challenges” ($r = .279$, $p < .01$) suggests that technological flaws are viewed in tandem with broader operational or compliance issues.

The “Effectiveness of Cybersecurity Frameworks” construct displays several moderate positive correlations, most prominently with “Classification of Major Cybersecurity Risks” ($r = .660$, $p < .01$) and “Organizational, Technical & Regulatory Challenges” ($r = .408$, $p < .01$). These relationships suggest that belief in the efficacy of cybersecurity frameworks increases when there is both clarity about the nature of cybersecurity threats and awareness of institutional or systemic barriers. The framework’s correlation with “Governmental & Industrial Preparedness” ($r = .335$, $p < .01$) and “Cybersecurity Risk Management” ($r = .379$, $p < .01$) implies that frameworks are perceived as integral to both sectoral readiness and risk mitigation. Correlations with “Technological Vulnerabilities” and “Targeted Cyberattacks” ($r = .241$, $p < .05$ for both) reflect a moderate association, indicating that although frameworks address these issues, respondents may see them as only partially effective in directly countering technical threats or malicious intrusions.

As noted, “Targeted Cyberattacks” correlates perfectly with “Technological Vulnerabilities” ($r = 1.000$, $p < .01$), underscoring their indistinguishability within the data. It also correlates moderately with “Organizational, Technical & Regulatory Challenges” ($r = .279$, $p < .01$), “Governmental & Industrial Preparedness” ($r = .357$, $p < .01$), and “Cybersecurity Risk Management” ($r = .355$, $p < .01$). These associations suggest that exposure to targeted attacks prompts a greater recognition of systemic weaknesses and the necessity for institutional and strategic preparedness. The correlation with “Effectiveness of Cybersecurity Frameworks” ($r = .241$, $p < .05$) supports the view that formalized security structures are moderately trusted to mitigate such attacks.

The strongest correlations in the matrix appear among the constructs “Organizational, Technical & Regulatory Challenges,” “Governmental & Industrial Preparedness,” and “Cybersecurity Risk Management.” Specifically, the correlation between “Organizational, Technical & Regulatory Challenges” and “Cybersecurity Risk Management” is very high ($r = .852$, $p < .01$), suggesting that respondents who perceive significant operational and regulatory challenges also emphasize structured approaches to risk management. Likewise, its correlation with “Governmental & Industrial Preparedness” is similarly high ($r = .842$, $p < .01$), indicating a perceived synergy between institutional preparedness and the mitigation of systemic cybersecurity challenges. The near-perfect correlation between “Governmental &

Industrial Preparedness" and "Cybersecurity Risk Management" ($r = .976$, $p < .01$) signifies that these constructs are almost indistinguishably linked in the minds of respondents. This strong association underscores a prevailing belief that coordinated efforts between government and industry are central to comprehensive cybersecurity risk management strategies.

4.3 Results

Hypothesis 01 – Classification of major cybersecurity risks has a positive influence on cybersecurity risk management in emerging technologies.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.219[a]	.048	.038	.86220

a. Predictors: (Constant), CLASSIFICATION OF MAJOR CYBERSECURITY RISKS

The model summary table provides a detailed statistical evaluation of the predictive relationship between the independent variable "Classification of Major Cybersecurity Risks" and the dependent variable, which is presumed to represent an aggregated measure of cybersecurity risk management effectiveness. The R value is 0.219, indicating a weak positive linear correlation between the predictor and the dependent variable. Although statistically significant in correlation analyses, this R value suggests that classification alone lacks sufficient strength to act as a sole predictor in a regression context. The R Square value of 0.048 further quantifies this relationship by indicating that only 4.8% of the variance in the dependent variable is explained by the classification of cybersecurity risks. This reflects a limited explanatory capacity, suggesting that most of the variation in cybersecurity outcomes is attributable to other factors not included in this model.

The Adjusted R Square, which accounts for the number of predictors and adjusts for sample size, is reported as 0.038. The reduction from the R Square value underscores the minimal contribution of the classification variable when used independently. This adjustment confirms that the variable's predictive utility is not substantial and that the observed explanatory power may be inflated due to chance. In empirical terms, this signifies that relying on risk classification as a standalone input fails to capture the complexity of cybersecurity dynamics in emerging technologies, which are typically shaped by a blend of technical, organizational, and strategic influences.

The standard error of the estimate is 0.86220, which reflects the average deviation of actual values from those predicted by the regression model. This comparatively high error term suggests that the data points are widely distributed around the regression line, which further suggests that the model's predictions are not accurate.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	3.654	1	3.654	4.916	.029[b]
	Residual	72.852	98	.743		
	Total	76.507	99			

a. Dependent Variable: CYBERSECURITY RISK MANAGEMENT

b. Predictors: (Constant), CLASSIFICATION OF MAJOR CYBERSECURITY RISKS

In order to determine the predictive impact of the independent variable, "Classification of Major Cybersecurity Risks," on the dependent variable, "Cybersecurity Risk Management," the ANOVA table provides a statistical analysis of the regression model. The percentage of the total variance in the dependent variable that can be accounted for by the predictor is represented by the regression sum of squares, which is given as 3.654. This number shows that the classification of key cybersecurity risks accounts for just a tiny percentage of the variation in cybersecurity risk management when compared to the entire sum of squares (76.507). Most of the variability left unaccounted for by the model is reflected in the residual sum of squares, which is 72.852 and accounts for 70% of the unaccounted variance.

The degrees of freedom (df) associated with the regression model are 1, corresponding to the single predictor variable used in the analysis, and the residual degrees of freedom are 98. The mean square values are calculated by dividing the sum of squares by their respective degrees of freedom. The regression mean square is 3.654, and the residual mean square is 0.743. These values are used to compute the F-statistic, which serves as a test of the overall significance of the regression model.

The F-value is 4.916, which reflects the ratio of the variance explained by the model to the variance unexplained. This value exceeds the critical threshold for statistical significance at the 0.05 level, as evidenced by the corresponding p-value of 0.029. The significance value ($p < .05$) confirms that the regression model, despite explaining a limited amount of variance, is statistically significant. This indicates that the classification of major cybersecurity risks contributes meaningfully, albeit modestly, to predicting cybersecurity risk management.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	3.110	.283		11.009	.000
	CLASSIFICATION OF MAJOR CYBERSECURITY RISKS	.193	.087	.219	2.217	.029

a. Dependent Variable: CYBERSECURITY RISK MANAGEMENT

The coefficients table provides detailed insight into the specific contribution of the independent variable, “Classification of Major Cybersecurity Risks,” to the prediction of the dependent variable, “Cybersecurity Risk Management,” within the regression model. The unstandardized coefficient (B) for the constant term is 3.110 with a standard error of 0.283. This constant represents the expected mean value of cybersecurity risk management when the classification score is zero, which serves as the model's baseline. The high t-value of 11.009 associated with the constant and its significance level of 0.000 indicate that this intercept is statistically significant and meaningfully different from zero, confirming the validity of the model's baseline estimate.

The unstandardized coefficient (B) for the predictor variable is 0.193, with a standard error of 0.087. This coefficient reflects the magnitude of change in the dependent variable, cybersecurity risk management, for each one-unit increase in the classification of cybersecurity risks. Specifically, for every one-point increase in classification score on the Likert scale, the expected score for cybersecurity risk management increases by 0.193 units. This positive coefficient indicates a direct relationship, whereby higher perceived clarity or awareness in classifying cybersecurity risks is associated with stronger perceptions or practices of cybersecurity risk management.

The standardized coefficient (Beta) is reported as 0.219. This value indicates the strength of the relationship in standardized units, allowing for comparisons across variables measured on different scales. A Beta of 0.219 signifies a modest but positive influence of classification on cybersecurity risk management, supporting the interpretation that improved risk classification contributes to better implementation or understanding of cybersecurity risk mitigation strategies.

The associated t-value for the classification variable is 2.217, and the significance level (p-value) is 0.029. Since this p-value is less than the 0.05 threshold, it confirms that the coefficient is statistically significant. This means that the relationship between classification and cybersecurity risk management is not due to random chance and holds true within the context of the sample studied. The statistical significance reinforces that classification of cybersecurity risks plays a meaningful role, though not a dominant one, in shaping cybersecurity risk management practices in emerging technology environments.

Hypothesis 02 – Technological vulnerabilities have a negative influence on cybersecurity risk management in emerging technologies.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.355[a]	.126	.117	.82589

a. Predictors: (Constant), TECHNOLOGICAL VULNERABILITIES

The model summary table presents a detailed statistical overview of the regression analysis conducted to assess the impact of the independent variable “Technological Vulnerabilities” on the dependent variable “Cybersecurity Risk Management” within the context of emerging technologies. The R value, representing the Pearson correlation coefficient between the predictor and the outcome variable, is 0.355. This indicates a moderate positive linear relationship, suggesting that as technological vulnerabilities increase in perceived importance or severity, cybersecurity risk management practices are also likely to improve or intensify in response.

The R Square value, which quantifies the proportion of variance in the dependent variable explained by the predictor, is 0.126. This implies that 12.6% of the variability in cybersecurity risk management can be attributed to technological vulnerabilities alone. Although this figure does not represent a large percentage, it reflects a meaningful level of explanatory power, particularly given the complex and multi-dimensional nature of cybersecurity in emerging technology environments. The result suggests that organizations or individuals who recognize and assess technological vulnerabilities are somewhat better equipped to manage cybersecurity risks, although much of the variance in risk management remains influenced by other unexamined factors.

The Adjusted R Square value is reported as 0.117, slightly lower than the R Square, and this adjustment accounts for the number of predictors and the sample size. The marginal decrease from 0.126 to 0.117 suggests minimal overfitting and reinforces that the predictor's contribution to the model is not artificially inflated. The adjusted value confirms that "Technological Vulnerabilities" contributes independently and modestly to explaining the variation in cybersecurity risk management, even when adjusting for model complexity.

The standard error of the estimate is 0.82589, which represents the average distance between observed values and the regression line. This relatively moderate standard error indicates a reasonable dispersion of actual values around predicted ones, reflecting some predictive accuracy but also notable variability. The dispersion reinforces that while technological vulnerabilities are a statistically meaningful predictor, they do not offer a comprehensive predictive model on their own, highlighting the multifaceted influences on effective cybersecurity risk management in the landscape of emerging technologies.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	9.661	1	9.661	14.163	.000[b]
	Residual	66.846	98	.682		
	Total	76.507	99			

a. Dependent Variable: CYBERSECURITY RISK MANAGEMENT
b. Predictors: (Constant), TECHNOLOGICAL VULNERABILITIES

The ANOVA table provides a comprehensive statistical assessment of the regression model, evaluating the predictive relationship between the independent variable "Technological Vulnerabilities" and the dependent variable "Cybersecurity Risk Management" within the domain of emerging technologies. The regression sum of squares is 9.661, indicating the amount of variation in the dependent variable that can be explained by the independent variable. This figure is substantial relative to the total sum of squares, which is 76.507, suggesting that "Technological Vulnerabilities" accounts for a measurable portion of the total variance in cybersecurity risk management.

The df associated with the regression model is 1, reflecting the inclusion of a single independent variable in the model, and the residual degrees of freedom are 98. These degrees of freedom form the basis for computing the mean square values. The mean square for the

regression is 9.661, while the residual mean square, representing the average unexplained variance, is 0.682. The comparatively larger value of the regression mean square indicates that the model explains a significant portion of the variation in the dependent variable relative to the error term.

The F-statistic, calculated as the ratio of the regression mean square to the residual mean square, is 14.163. This value is considerably greater than the critical F-value required for significance at the 0.05 level, suggesting that the overall regression model is statistically significant. The associated significance value (p = 0.000) further confirms this, indicating that the probability of observing such an F-statistic by random chance is extremely low. As a result, the null hypothesis, that there is no linear relationship between technological vulnerabilities and cybersecurity risk management, is rejected.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.498	.332		7.531	.000
	TECHNOLOGICAL VULNERABILITIES	.399	.106	.355	3.763	.000

a. Dependent Variable: CYBERSECURITY RISK MANAGEMENT

The coefficients table outlines the regression parameters used to evaluate the influence of the independent variable “Technological Vulnerabilities” on the dependent variable “Cybersecurity Risk Management.” The unstandardized coefficient for the constant is 2.498 with a standard error of 0.332. This constant indicates the predicted baseline level of cybersecurity risk management when the value of technological vulnerabilities is zero. The associated t-value for the constant is 7.531, and the significance level (p = .000) indicates that the intercept is statistically significant, validating that the base level of the dependent variable is meaningfully different from zero in the absence of technological vulnerabilities.

The B for the technological vulnerabilities is 0.399, with a standard error of 0.106. This coefficient signifies that for every one-unit increase in the perception or rating of technological vulnerabilities (as measured on the Likert scale), the expected increase in cybersecurity risk management is 0.399 units. This reflects a moderately strong and positive

linear relationship, suggesting that a higher acknowledgment of technological vulnerabilities, such as outdated protocols, system weaknesses, or insufficient threat detection capabilities, leads to increased focus or improvement in managing cybersecurity risks.

The Beta value is 0.355, which reflects the relative strength of the predictor in standard deviation units. This value indicates that technological vulnerabilities have a moderate effect on cybersecurity risk management compared to other potential predictors. The positive Beta confirms that as the importance or severity of technological vulnerabilities rises, so too does the emphasis placed on structured risk management strategies, indicating a reactive alignment of security practices with evolving system-level threats.

The t-value associated with the technological vulnerabilities is 3.763, which exceeds the typical threshold for significance, and the corresponding p-value is 0.000. This significance level demonstrates that the observed relationship is not due to random chance and that technological vulnerabilities exert a statistically significant influence on the dependent variable. The low standard error combined with a high t-value reinforces the precision and reliability of the coefficient estimate.

Hypothesis 03 – Effectiveness of cybersecurity frameworks has a positive influence on cybersecurity risk management in emerging technologies.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.379[a]	.144	.135	.81756

a. Predictors: (Constant), EFFECTIVENESS OF CYBERSECURITY FRAMEWORKS

The model summary table presents key statistical indicators of the linear regression analysis conducted to assess the relationship between the independent variable “Effectiveness of Cybersecurity Frameworks” and the dependent variable “Cybersecurity Risk Management” within the context of emerging technologies. The R value of 0.379 represents the Pearson correlation coefficient, indicating a moderate positive linear relationship between the two variables. This suggests that as the perceived effectiveness of cybersecurity frameworks increases, the level of cybersecurity risk management practices also tends to improve. This relationship reflects the logical alignment where robust frameworks contribute positively to risk management strategies.

The R Square value is reported as 0.144, indicating that approximately 14.4% of the variance in cybersecurity risk management is explained by the perceived effectiveness of cybersecurity frameworks. Although the proportion is modest, it is meaningful in the context of cybersecurity, where multiple variables contribute to overall risk management outcomes. The finding suggests that organizations that implement effective frameworks, such as NIST, ISO/IEC 27001, or other regulatory or compliance-driven architectures, demonstrate improved cybersecurity governance and response capabilities.

The adjusted R Square value is 0.135, which accounts for the number of predictors in the model and adjusts for potential overfitting due to sample size. The slight reduction from the R Square reflects a minimal correction, affirming the model's stability and its validity in explaining the dependent variable. Even when model complexity is taken into account, the adjusted value confirms that "Effectiveness of Cybersecurity Frameworks" is a consistent and trustworthy predictor of cybersecurity risk management.

The average departure of the actual data values from the anticipated regression line is represented by the standard error of the estimate, which is 0.81756. A respectable degree of prediction accuracy inside the model is shown by this standard error, which is rather moderate. It implies that even if "Effectiveness of Cybersecurity Frameworks" plays a major role in forecasting cybersecurity risk management procedures, there is still variability that cannot be explained by this one prediction alone.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	11.003	1	11.003	16.462	.000[b]
	Residual	65.504	98	.668		
	Total	76.507	99			

a. Dependent Variable: CYBERSECURITY RISK MANAGEMENT

b. Predictors: (Constant), EFFECTIVENESS OF CYBERSECURITY FRAMEWORKS

The ANOVA table provides an in-depth statistical evaluation of the regression model, exploring the predictive impact of the independent variable “Effectiveness of Cybersecurity Frameworks” on the dependent variable “Cybersecurity Risk Management” within the context of emerging technologies. The regression sum of squares is reported as 11.003, indicating the portion of variance in cybersecurity risk management that can be attributed to variations in the perceived effectiveness of cybersecurity frameworks. This value is

significant when compared to the total sum of squares, which is 76.507, implying that the model explains a considerable proportion of the overall variance in the dependent variable.

The model includes one predictor variable, as indicated by the degrees of freedom (df) for regression being 1, and the residual degrees of freedom are 98. The mean square for the regression is equivalent to the regression sum of squares divided by its degrees of freedom, yielding a value of 11.003. The residual mean square, representing the average unexplained variance, is 0.668, calculated by dividing the residual sum of squares (65.504) by its degrees of freedom (98). The comparison of these mean squares forms the basis for calculating the F-statistic.

The F-value is 16.462, which is significantly higher than the critical value typically required to declare statistical significance at the 0.05 level. This high F-statistic strongly suggests that the regression model provides a better fit to the data than a model with no predictors. The associated p-value (Sig.) is .000, which further confirms the statistical significance of the model. This indicates that the probability of observing such a strong F-value due to chance is less than 0.001, thereby validating the hypothesis that "Effectiveness of Cybersecurity Frameworks" significantly influences cybersecurity risk management.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.652	.273		9.731	.000
	EFFECTIVENESS OF CYBERSECURITY FRAMEWORKS	.334	.082	.379	4.057	.000

a. Dependent Variable: CYBERSECURITY RISK MANAGEMENT

The coefficients table offers a detailed interpretation of the linear regression analysis examining the effect of the independent variable, "Effectiveness of Cybersecurity Frameworks," on the dependent variable, "Cybersecurity Risk Management," within the domain of emerging technology. The unstandardized coefficient for the constant is 2.652 with a standard error of 0.273. This value represents the baseline level of cybersecurity risk management when the predictor variable, effectiveness of cybersecurity frameworks, is zero. The high t-value of 9.731 and the significance level of .000 indicate that the intercept is

statistically significant and not due to chance, affirming the model's reliability at its base level.

The unstandardized coefficient for "Effectiveness of Cybersecurity Frameworks" is 0.334 with a standard error of 0.082. This coefficient implies that for every one-unit increase in the effectiveness of cybersecurity frameworks, as perceived or rated by respondents, there is an expected increase of 0.334 units in the level of cybersecurity risk management. This relationship is both direct and positive, signifying that organizations or institutions that rate their cybersecurity frameworks as more effective are likely to also report stronger engagement in risk management activities. These may include proactive threat detection, incident response readiness, compliance monitoring, and robust recovery mechanisms.

The Beta value is 0.379, indicating the strength of the relationship in terms of standard deviations. This figure suggests a moderately strong predictive effect of the independent variable on the dependent one. Specifically, a one standard deviation increase in the perceived effectiveness of cybersecurity frameworks corresponds to a 0.379 standard deviation increase in cybersecurity risk management practices. The t-value of 4.057 for the predictor variable confirms the statistical significance of this relationship, and the associated p-value of .000 further affirms that the effect observed is not due to random variation. The low standard error reinforces the precision of the estimate, ensuring reliability in the findings.

Hypothesis 04 – Targeted cyberattacks have a negative influence on cybersecurity risk management in emerging technologies.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.355[a]	.126	.117	.82589

a. Predictors: (Constant), TARGETED CYBERATTACKS

The model summary table presents the statistical strength and explanatory power of a simple linear regression model that investigates the influence of the independent variable "Targeted Cyberattacks" on the dependent variable "Cybersecurity Risk Management" in the context of emerging technology environments. The Pearson correlation coefficient is recorded at 0.355, indicating a moderate positive relationship between the two variables. This value suggests that as the frequency, severity, or perceived threat of targeted cyberattacks increases, there is

a corresponding increase in the application or intensity of cybersecurity risk management practices within organizations.

The R Square value, also known as the coefficient of determination, is 0.126. This metric quantifies the proportion of variance in the dependent variable that can be explained by the independent variable. In this model, 12.6% of the variability in cybersecurity risk management can be attributed to variations in the exposure to or perception of targeted cyberattacks. While this percentage does not indicate a dominant predictor, it is statistically meaningful in the context of behavioral and organizational studies, where multiple complex factors typically influence decision-making and operational strategies.

The adjusted R Square, which accounts for the number of predictors and adjusts for potential overfitting in small samples, is slightly lower at 0.117. This slight reduction confirms that the explanatory power of the model is not inflated and remains consistent when generalized to the broader population beyond the sampled data. The standard error of the estimate is 0.82589, representing the average distance that the observed values fall from the regression line. This relatively moderate standard error indicates a reasonable level of prediction accuracy, with less than one unit of deviation on average between observed and predicted values of cybersecurity risk management.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	9.661	1	9.661	14.163	.000[b]
	Residual	66.846	98	.682		
	Total	76.507	99			

a. Dependent Variable: CYBERSECURITY RISK MANAGEMENT
b. Predictors: (Constant), TARGETED CYBERATTACKS

The ANOVA table provides statistical validation for the regression model that assesses the impact of the independent variable “Targeted Cyberattacks” on the dependent variable “Cybersecurity Risk Management” in the context of emerging technologies. The regression sum of squares is reported at 9.661 with 1 degree of freedom, indicating the amount of variability in cybersecurity risk management that is explained by the predictor variable, targeted cyberattacks. This figure reflects a notable portion of the model’s explanatory capacity, reinforcing that the model captures a meaningful relationship between the two variables.

The residual sum of squares is 66.846 with 98 degrees of freedom, representing the unexplained variance, i.e., the portion of variation in cybersecurity risk management that is due to other factors not included in the model. The total sum of squares, which is the combination of regression and residual sums, stands at 76.507 across 99 degrees of freedom, capturing the overall variability in the outcome variable. These values confirm that the model accounts for a measurable and statistically significant portion of the total variance.

The mean square values are obtained by dividing the sum of squares by their respective degrees of freedom. For the regression, the mean square is 9.661, and for the residuals, it is 0.682. The F-ratio, calculated as the mean square regression divided by the mean square residual, is 14.163. This F-statistic evaluates whether the regression model provides a better fit to the data than a model without the independent variable. The significance value (Sig.) is reported as .000, which is far below the conventional alpha threshold of 0.05. This p-value confirms that the regression model is statistically significant, and the likelihood that the observed relationship occurred by chance is extremely low.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.498	.332		7.531	.000
	TARGETED CYBERATTACKS	.399	.106	.355	3.763	.000

a. Dependent Variable: CYBERSECURITY RISK MANAGEMENT

The coefficients table presents the regression analysis results evaluating the influence of "Targeted Cyberattacks" on "Cybersecurity Risk Management" within the context of emerging technologies. The unstandardized coefficient for the constant term is 2.498, with a standard error of 0.332. This intercept represents the predicted value of cybersecurity risk management when the independent variable, targeted cyberattacks, is zero. The corresponding t-value of 7.531 and significance level ($p = 0.000$) confirm that this intercept is statistically significant, establishing a reliable baseline for the regression model.

The unstandardized coefficient for targeted cyberattacks is 0.399, with a standard error of 0.106. This coefficient indicates that for every one-unit increase in the perception or frequency of targeted cyberattacks, the cybersecurity risk management score is expected to

increase by 0.399 units, holding all else constant. This positive coefficient suggests a direct and moderate relationship where an increase in targeted cyberattacks correlates with improved or heightened risk management measures, possibly reflecting reactive or adaptive responses by organizations.

The Beta for targeted cyberattacks is 0.355, indicating the strength of this predictor relative to other variables when measured on a common scale. A Beta value of 0.355 suggests a moderate effect size, meaning targeted cyberattacks have a meaningful but not overwhelming influence on cybersecurity risk management outcomes. The t-statistic associated with targeted cyberattacks is 3.763, with a p-value of 0.000, which is well below the typical 0.05 threshold. This confirms that the relationship between targeted cyberattacks and cybersecurity risk management is statistically significant and unlikely to be due to chance.

Hypothesis 05 – Organizational, technical, and regulatory challenges have a negative influence on cybersecurity risk management in emerging technologies.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.852[a]	.727	.724	.46190

a. Predictors: (Constant), ORGANIZATIONAL, TECHNICAL, & REGULATORY CHALLENGES

The model summary table presents key statistical measures that assess the strength and explanatory power of the regression model predicting “Cybersecurity Risk Management” based on the independent variable “Organizational, Technical, and Regulatory Challenges.” The R is notably high at 0.852, reflecting a strong positive association between these challenges and cybersecurity risk management practices in the context of emerging technologies. This correlation indicates that as organizations face increasing difficulties in organizational structure, technical complexity, and regulatory compliance, their engagement with cybersecurity risk management intensifies accordingly.

The coefficient of determination, R Square, is 0.727, signifying that approximately 72.7% of the variance in cybersecurity risk management can be explained by the combined effects of organizational, technical, and regulatory challenges. This represents a substantial explanatory power, illustrating that these challenges are critical determinants shaping how organizations respond to cybersecurity risks in emerging technology environments.

The model's number of predictors and sample size are taken into consideration to prevent overfitting, resulting in a somewhat lower adjusted R Square of 0.724. The model's robustness is confirmed by the little difference between R Square and adjusted R Square, which also implies that the high explanatory power is not a result of artificial inflation. This modification strengthens the model's prediction power's applicability to comparable populations or environments in cybersecurity studies. The average difference between the regression model's predicted values and the actual values is measured by the estimate's standard error, which is 0.46190. This comparatively low standard error suggests that the residuals (or mistakes) are minimal and that the model's predictions are correct. Based on the organizational, technological, and regulatory issues encountered, this implies excellent dependability in calculating cybersecurity risk management.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	55.598	1	55.598	260.596	.000[b]
	Residual	20.908	98	.213		
	Total	76.507	99			

a. Dependent Variable: CYBERSECURITY RISK MANAGEMENT

b. Predictors: (Constant), ORGANIZATIONAL, TECHNICAL & REGULATORY CHALLENGES

The ANOVA table provides a thorough evaluation of the overall importance of the regression model by analyzing how well "Organizational, Technical, and Regulatory Challenges" forecast changes in "Cybersecurity Risk Management" in contexts including developing technologies. At 55.598 with 1 df, the regression sums of squares, which shows how much of the variation in cybersecurity risk management is attributable to the predictor variable, is noticeably high. This high value demonstrates how organizational, technological, and legal obstacles have a significant explanatory power when it relates to accounting for shifts in cybersecurity management approaches.

The residual sum of squares, measuring unexplained variance, is 20.908 with 98 degrees of freedom. This residual variance reflects the portion of cybersecurity risk management that remains unexplained by the model, potentially due to other unmeasured factors or random error. The total sum of squares, combining regression and residual sums, is 76.507 across 99 degrees of freedom, representing the total variability observed in cybersecurity risk management within the sample.

The regression means square equals 55.598, while the residual mean square is substantially lower at 0.213. The F-statistic, calculated as the ratio of regression mean square to residual mean square, is an exceptionally high 260.596. This large F-value suggests that the regression model explains significantly more variance than would be expected by chance alone, highlighting the strong predictive capacity of organizational, technical, and regulatory challenges on cybersecurity risk management. The significance value (Sig.) is reported as .000, indicating a p-value well below the conventional alpha level of 0.05. This confirms the statistical significance of the model, reinforcing that the relationship between the independent variable and cybersecurity risk management is unlikely to be due to random variation.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.810	.185		4.369	.000
	ORGANIZATIONAL, TECHNICAL & REGULATORY CHALLENGES	.789	.049	.852	16.143	.000

a. Dependent Variable: CYBERSECURITY RISK MANAGEMENT

The regression model that uses "Organizational, Technical, and Regulatory Challenges" as the independent variable to predict "Cybersecurity Risk Management" is explained in detail in the coefficients table. With a standard error of 0.185 and an unstandardized constant value of 0.810, the t-value is 4.369 and the significance level is set at.000. Accordingly, the baseline state of cybersecurity risk management is assessed to be 0.810 on the measured scale when the predictor variable, regulatory, technological, and organizational challenges, is zero. Even in the absence of difficulties, a basic level of cybersecurity management is evident from the statistically significant intercept, most likely as a result of ingrained corporate policies or pre-existing security procedures.

The unstandardized coefficient for “Organizational, Technical, and Regulatory Challenges” is 0.789, accompanied by a very small standard error of 0.049. This coefficient quantifies the expected change in cybersecurity risk management for each one-unit increase in the

combined measure of organizational, technical, and regulatory challenges. Specifically, for every incremental increase in these challenges, the cybersecurity risk management score increases by 0.789 units. This substantial coefficient reflects a strong positive influence of the predictor variable on the outcome, suggesting that as organizations encounter more complex or stringent challenges, their cybersecurity management efforts intensify proportionally.

A Beta of 0.852 highlights that “Organizational, Technical, and Regulatory Challenges” is a dominant predictor of cybersecurity risk management in this model, explaining a significant portion of the variance. The t-value of 16.143 for the challenges predictor is exceptionally high, coupled with a significance (Sig.) level of .000, indicating that the predictor’s effect is statistically significant beyond conventional thresholds. This strongly supports the reliability and validity of the model’s predictive capacity, reinforcing the critical role that organizational, technical, and regulatory challenges play in shaping cybersecurity risk management strategies within emerging technology environments.

Hypothesis 06 – Governmental and industrial preparedness has a positive influence on cybersecurity risk management in emerging technologies.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.976[a]	.952	.952	.19277

a. Predictors: (Constant), GOVERNMENTAL & INDUSTRIAL PREPAREDNESS

The model summary table presents critical statistics evaluating the regression analysis where "Governmental & Industrial Preparedness" serves as the predictor variable for "Cybersecurity Risk Management" within the context of emerging technologies. The R is reported as 0.976, indicating an exceptionally strong positive linear relationship between the level of preparedness in governmental and industrial sectors and the effectiveness or extent of cybersecurity risk management. This near-perfect correlation suggests that as preparedness increases, cybersecurity risk management improves proportionally, demonstrating the integral role that readiness at these systemic levels plays in shaping cybersecurity outcomes.

The R Square is 0.952, which signifies that approximately 95.2% of the variance in cybersecurity risk management can be explained by variations in governmental and industrial preparedness. This remarkably high R Square value highlights the predictor’s dominant explanatory power, suggesting that governmental policies, regulatory frameworks, industrial

compliance, and readiness protocols are critical determinants in the management of cybersecurity risks. Such a high percentage of explained variance underscores that preparedness in these sectors is a fundamental factor driving cybersecurity effectiveness, overshadowing other potential influences.

Adjusted R Square, reported at 0.952, closely aligns with R Square, indicating that the model maintains its strong explanatory power after adjusting for the number of predictors and sample size. This minimal difference between R Square and Adjusted R Square reflects the model's robustness and that it is not overfitted, reinforcing the reliability of the results in representing the true relationship within the population. The estimate's standard error, which quantifies the average separation between observed values and the regression line, is 0.19277. A comparatively low standard error shows accurate predictions and little residual error, indicating that the expected outcomes for cybersecurity risk management roughly correspond to the actual observed data points.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	72.865	1	72.865	1960.860	.000[b]
	Residual	3.642	98	.037		
	Total	76.507	99			

a. Dependent Variable: CYBERSECURITY RISK MANAGEMENT

b. Predictors: (Constant), GOVERNMENTAL & INDUSTRIAL PREPAREDNESS

A comprehensive evaluation of the regression model's general significance and explanatory power, where "Governmental & Industrial Preparedness" predicts "Cybersecurity Risk Management," is shown in the ANOVA table. Governmental and industrial preparation is the predictor variable that accounts for 72.865 of the variation in cybersecurity risk management, according to the regression sum of squares (SSR). Given that the total sum of squares (SST) is 76.507, this implies that a substantial proportion of the total variability in cybersecurity risk management outcomes is attributable to differences in governmental and industrial readiness.

The residual sum of squares (SSE) is reported as 3.642, which quantifies the variance in cybersecurity risk management that remains unexplained by the model. This relatively low residual sum of squares compared to the regression sum of squares indicates that the model accounts for the vast majority of variation in the outcome variable, leaving minimal unexplained error. The df for regression is 1, reflecting that a single predictor variable is

included in the model. The residual degrees of freedom are 98, corresponding to the sample size minus the number of parameters estimated (N – k – 1).

The mean square for regression (MSR), calculated as SSR divided by its degrees of freedom, is 72.865. The mean square for residuals (MSE), the ratio of SSE to its degrees of freedom, is 0.037. The F-statistic is an exceptionally high 1960.860, calculated by dividing MSR by MSE, which measures how much more variance is explained by the model than would be expected by chance. The significance value (Sig.) of .000 is well below the conventional alpha levels (e.g., 0.05), demonstrating that the regression model is statistically significant. This indicates that the predictor variable, governmental and industrial preparedness, provides a significant contribution to explaining variance in cybersecurity risk management.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.222	.081		2.738	.007
	GOVERNMENTAL & INDUSTRIAL PREPAREDNESS	.950	.021	.976	44.282	.000

a. Dependent Variable: CYBERSECURITY RISK MANAGEMENT

The coefficients table presents detailed information regarding the regression coefficients of the model predicting “Cybersecurity Risk Management” using “Governmental & Industrial Preparedness” as the independent variable. The B for the constant term is 0.222 with a standard error of 0.081. This intercept represents the estimated value of cybersecurity risk management when the level of governmental and industrial preparedness is zero. Although a zero level of preparedness may be hypothetical, the intercept provides a baseline reference point from which changes due to preparedness are measured. The associated t-value of 2.738 and significance level ($p = 0.007$) indicate that the intercept is statistically significantly different from zero, confirming the model’s validity and foundation.

The unstandardized coefficient for the predictor “Governmental & Industrial Preparedness” is 0.950 with a very small standard error of 0.021, indicating a precise estimate of the slope. This coefficient reflects that for every one-unit increase in governmental and industrial preparedness, the cybersecurity risk management score increases by 0.950 units, holding

other factors constant. This nearly one-to-one increase suggests a highly proportional and direct influence of preparedness on improving cybersecurity risk management practices. The narrow standard error underscores the reliability and stability of this estimated effect

The Beta value is 0.976, which further emphasizes the strength of the relationship by expressing the coefficient in standardized units. This value, being very close to 1, implies that governmental and industrial preparedness is a dominant predictor variable exerting a substantial impact on cybersecurity risk management, relative to other potential factors not included in the model. The t-statistic for the preparedness variable is extremely high at 44.282, which indicates a highly significant predictive effect, supported by the p-value of .000 (less than 0.001). This confirms that the relationship between preparedness and cybersecurity risk management is not due to random chance but is a robust and statistically significant association.

4.4 Summary of Hypothesis

Research Hypothesis	***Result (Accepted or Rejected)***
Classification of major cybersecurity risks has a positive influence on cybersecurity risk management in emerging technologies.	**Accepted**
Technological vulnerabilities have a negative influence on cybersecurity risk management in emerging technologies.	**Accepted**
Effectiven**ess** of cybersecurity frameworks has a positive influence on cybersecurity risk management in emerging technologies.	**Accepted**
Targeted cyberattacks have a negative influence on cybersecurity risk management in emerging technologies.	**Accepted**
Organizational, technical, and regulatory challenges have a negative influence on cybersecurity risk management in emerging technologies.	**Accepted**

Governmental and industrial preparedness has a positive influence on cybersecurity risk management in emerging technologies.	**Accepted**

5. CHAPTER 05 – DISCUSSION & RECOMMENDATION

5.1 Discussion of Results & Findings

5.1.1.1 Classification of major cybersecurity risks has a positive influence on cybersecurity risk management in emerging technologies.

A first step toward improving risk management within the framework of developing technologies is the classification of cybersecurity hazards. To facilitate the implementation of specialized security mechanisms, this process entails identifying, classifying, and assessing certain risks pertinent to each technological area, whether it be cloud computing, blockchain, IoT, or AI. Arora et al. (2024) point out that a structured four-tiered architecture for IoT risk management, which covers hazards at the network, device, application, and user levels, allows for detailed analysis and resource allocation priority. In the absence of such taxonomies, security efforts are frequently misdirected, either ignoring high-impact sectors or overprotecting low-risk components. According to the literature, the lack of a clear classification leads to reactive and dispersed cybersecurity strategies, particularly in settings like smart cities and industrial IoT.

The significance of risk classification in blockchain ecosystems is also emphasized by Alfandi et al. (2021), where risks originate from consensus vulnerabilities, smart contract logic errors, and key mismanagement. By categorizing these dangers, domain-specific technologies like formal verification and zero-knowledge proofs may be applied more effectively. Because classification draws attention to the systematic architecture of risk, it actively influences operational strategy rather than just supporting academic rigor. For instance, Möller (2023) points out that regular risks need to be clearly categorized to guarantee that the appropriate mitigation procedures are triggered. This is demonstrated by the frequent exploitation of improperly setup S3 buckets within cloud systems.

Additionally, categorization improves communication across sectors, allowing technical and non-technical stakeholders to comprehend, predict, and work together on risk management. Moreover, risk classification guides the creation of regulations and the benchmarking of compliance, particularly in multi-jurisdictional contexts like telemedicine and FinTech (Goudarzi et al., 2022). Therefore, an organized categorization system influences cybersecurity management in emerging technologies in a favourable way by establishing a feedback loop between risk identification, regulatory alignment, and effective defence implementation.

5.1.1.2 Technological vulnerabilities have a negative influence on cybersecurity risk management in emerging technologies.

Because they increase unpredictability, system vulnerability, and the speed at which threats may be exploited, technological vulnerabilities make cybersecurity risk management much more difficult. These weaknesses in developing technologies are systemic design flaws that attackers deliberately seek rather than just technical errors. According to Shafiq et al. (2022) and Almazarqi (2024), IoT devices frequently have limited processing power, out-of-date firmware, hardcoded passwords, and inadequate encryption algorithms. Due to these limitations, devices are always vulnerable to attack, as common security measures like intrusion detection and real-time patching cannot be implemented.

Likewise, adversarial inputs, data poisoning, and model inversion assaults can affect AI and machine learning systems (Goldblum et al., 2022; Schnitzer & Tiruwuha, 2024). These flaws compromise the accuracy of AI-driven detection systems and make them vulnerable to erroneous categorization or even takeover. Furthermore, forensic investigation and prompt remediation are further hampered by the fact that AI models frequently function as "black boxes." It is challenging to determine when a breach has taken place or how an attack vector was carried out because of these traits, which limit efficient risk assessment.

Because deployed code is immutable in blockchain contexts, smart contract vulnerabilities (such as re-entrancy issues or logic mistakes) produce persistent, irreversible attack surfaces (Scharfman, 2024). The DAO breach serves as an example of how badly drafted smart contracts may cause significant losses in terms of money and reputation. Attackers are motivated to thoroughly examine such contracts for zero-day logic problems since they are immutable and publicly available.

5.1.1.3 Effectiveness of cybersecurity frameworks has a positive influence on cybersecurity risk management in emerging technologies.

In order to coordinate and standardize security procedures across intricate technology ecosystems, cybersecurity frameworks are essential. Their efficacy has a direct impact on cybersecurity risk management's responsiveness, resilience, and robustness. Frameworks like ISO 27001, NIST, and sector-specific standards offer direction on how to recognize, safeguard, detect, respond to, and recover from cyber disasters in new technologies (NIST, 2018). However, the flexibility and uniqueness of these frameworks are critical to their efficacy in the context of developing technology.

Mekala et al. (2023) claim that standard frameworks in IIoT contexts do not provide operational-level direction on how to modify controls for decentralized, real-time, and data-intensive systems. For cybersecurity frameworks to be effective, they need to provide behavioral anomaly detection, AI-powered risk estimation, and continuous learning. AI-integrated SIEM systems are supported by Sania et al. (2024) because they complement current frameworks while offering contextual reaction to changing risks. This integration is a prime example of how technology augmentation improves framework efficacy.

Alfandi et al. (2021) contend that formal techniques for confirming smart contracts and cryptographic integrity are essential components of contemporary cybersecurity frameworks in the blockchain space. The logic-based vulnerabilities inherent in decentralized applications are not adequately addressed by conventional frameworks without these improvements. In order to guarantee traceability and regulatory compliance, Razdan and Sharma (2022) advise incorporating blockchain-driven authorization management systems into medical cybersecurity frameworks, especially for IoMT.

5.1.1.4 Targeted cyberattacks have a negative influence on cybersecurity risk management in emerging technologies.

Because targeted assaults undermine confidence, take advantage of flaws in particular systems, and avoid discovery, they provide particular challenges for cybersecurity risk management. Usually, highly skilled adversaries, such as insider threats, cybercriminal syndicates, and state-sponsored organizations, plan these attacks. Such breaches take use of embedded software flaws and supply chain dependencies, as demonstrated by the 2020 SolarWinds assault, which allows attackers to enter several high-value targets at once (Cordey, 2023).

Targeted assaults frequently use firmware flaws or default setups in IoT systems to obtain long-term access. For example, Mirai and its derivatives showed how attackers may methodically create botnets for DDoS attacks by using low-entropy credentials over thousands of machines (Almazarqi, 2024). These devices can be used as launching pads for more complex lateral assaults across linked infrastructures after they have been hacked.

AI systems are also susceptible to adversarial inputs that are precisely targeted, in which the attacker creates small perturbations that have the potential to significantly change the model's outputs. Such assaults might result in operational risks for autonomous systems, such misread traffic signals or incorrectly diagnosed medical pictures (Sarker, 2024).

Furthermore, AI-based threat detection is problematic since data poisoning attacks frequently target certain ML pipelines.

Targeted assaults in blockchain technology take advantage of smart contracts' permanence and predictability. According to Scharfman (2024), reentrancy vulnerabilities are found and exploited by meticulous code study and transaction simulations rather than by coincidence. This was evident in the DAO hack. The idea of unchangeable trust is challenged by these attacks, which are by their very nature targeted.

5.1.1.5 Organizational, technical, and regulatory challenges have a negative influence on cybersecurity risk management in emerging technologies.

In the dynamic world of developing technologies, organizational, technological, and regulatory obstacles significantly impair cybersecurity risk management's efficacy. The pervasive skills gap is one of the most urgent constraints from an organizational standpoint. Ineffective incident response, incorrect configurations, and an excessive dependence on legacy tools are caused by the lack of skilled cybersecurity professionals, especially those who can comprehend the complicated risks posed by AI, IoT, and blockchain systems (Mekala et al., 2023; Möller, 2023). Due to their lack of dedicated security teams, SMEs and government organizations are particularly susceptible to cyberattacks coming from new technological platforms.

The technological integration of autonomous, decentralized, and real-time systems presents difficulties for conventional security concepts. For example, edge computing creates settings that are susceptible to delay, making standard procedures like identity management or centralized threat detection impractical (Bhushan et al., 2021). There are still issues with adversarial resistance in AI and the technical difficulty of smart contract authentication in blockchain systems (Alfandi et al., 2021; Goldblum et al., 2022). These limitations postpone real-time risk mitigation and impede proper risk modeling. These problems are further made worse by regulatory fragmentation. According to Goudarzi et al. (2022), new technologies often operate in industries and legal systems with disparate regulations.

5.1.1.6 Governmental and industrial preparedness has a positive influence on cybersecurity risk management in emerging technologies.

The effectiveness of cybersecurity risk management is greatly increased by governmental and industry readiness, which makes it possible for preemptive threat mitigation, organized

response to incidents, and optimistic policy design that takes into account developing technology. According to studies, implementing security-by-design frameworks, ensuring regulatory harmonization, and making investments in cyber resilience infrastructure are all part of institutional preparation. For instance, in complicated jurisdictions dealing with cloud, blockchain, and quantum systems, government initiatives like national cybersecurity policies or AI-specific rules aid in the creation of consistent compliance settings (Razdan & Sharma, 2022; Goudarzi et al., 2022).

When properly matched with legislative frameworks, industrial readiness also increases the ability to defend against cyberattacks. The detection of lateral movements and zero-day threats is more successful for large businesses that have implemented modern technologies, such as SIEM (Security Information and Event Management) systems driven by artificial intelligence (Sania et al., 2024). To prevent sophisticated persistent attacks in critical infrastructure, such as IIoT and smart grid ecosystems, these businesses frequently use threat intelligence platforms and layered security architectures (Mekala et al., 2023). Additionally, simulation exercises, public-private cooperation, and worker training all demonstrate industrial preparedness.

5.2 Conclusion

The present research focuses on examining the different cybersecurity risks associated with the widespread use of emerging technologies, including AI, blockchain, the IoT, cloud computing, and quantum computing. It looked at these risks' characteristics, development, and mitigation using both theoretical models and actual research. The study found that conventional cybersecurity frameworks, such as the NIST Cybersecurity Framework and ISO 27001, are not flexible enough to handle the highly intelligent, decentralized, and interoperable characteristics of developing technologies. These frameworks are poor for managing risks in rapidly changing digital ecosystems because they are frequently broad, reactive, and context-insensitive.

The fact that emergent technologies have organizational, regulatory, and human-focused vulnerabilities in addition to technological ones was one of the most important discoveries. For example, model poisoning and adversarial assaults are threats to AI systems, and firmware flaws and inadequate authentication jeopardize IoT networks. The intrinsic opacity and immutability of blockchain smart contracts, as well as improperly designed cloud settings, accentuate these problems. According to the findings, integrating new technology

increases cybersecurity risks dramatically. For instance, AI-driven IoT systems that are implemented through cloud platforms have compounded vulnerabilities, indicating that an attack in one layer (such as cloud configuration) might compromise the confidentiality and integrity of the entire system. A multifaceted approach to risk management is required due to these interdependencies, as opposed to discrete technology-specific measures.

Particularly in underdeveloped countries, where cyber risk governance is dispersed, underfunded, and lacks cross-border interoperability, the study also validated the shortcomings of the present legal and regulatory frameworks. Exploitable gaps are created by this regulatory lag, particularly in technologies such blockchain and artificial intelligences, which operate naturally in decentralized and multinational environments. The creation of a technology-specific risk taxonomy and the suggestion of a multi-layered cybersecurity posture model with technical, operational, and strategic controls adapted to new technological contexts were two important contributions of this study. The research also emphasized the need for worldwide regulatory harmonization, skilled hiring and retention, and proactive policy frameworks for successful cybersecurity governance.

The study also emphasized how important it is to incorporate ethical risk concerns into cybersecurity governance frameworks, especially for technologies that have the ability to monitor or make decisions on their own, such biometric systems and drones driven by artificial intelligence. As demonstrated by empirical research, governments and businesses alike are ill-prepared for the scope and complexity of cyberthreats presented by new technology. Across industries, particularly in critical infrastructure and healthcare, the lack of scenario-based risk models, inadequate incident response preparedness, and a shortage of qualified staff were recurring themes.

This dissertation offers a contextualized, empirical, and multidisciplinary method for investigating cybersecurity risk management within emerging technologies, therefore addressing a substantial research need. Policymakers, regulators, cybersecurity experts, and engineers looking to strike a balance between innovation, security, and trust will find specific relevance in its findings and recommendations.

5.3 Implications of the Study

5.3.1 Theoretical Implications

Theoretically, this research significantly advances our understanding of cybersecurity threats in the context of newly emerging technologies like cloud computing, blockchain, AI, and

IoT. One of the main theoretical developments concerns the rethinking of risk perception in settings where the lines separating end users and technology systems are becoming more and more distorted. This research highlights the relationship dynamics between technology architecture and human risk cognition, in contrast to typical cybersecurity models that concentrate on perimeter protection and technological weaknesses. The increasing amount of research that emphasizes risk as a socio-technical construct impacted by perceived transparency, corporate culture, system complexity, and technological maturity is further supported by this work.

Additionally, the results indicate that current frameworks, such as the protection motivation theory (PMT) and the technology acceptance model, need to be improved to take into account the changing danger landscape presented by hyperconnected environments. For example, this study reveals that consumers consider perceived data management, algorithmic predictability, and compliance transparency in the context of cybersecurity, even while TAM takes into account perceived usefulness and simplicity of use. Therefore, by incorporating these variables within behavioral acceptance models, the study advances theory, especially for enterprise systems that use cloud infrastructure and artificial intelligence.

The study also improves the theoretical foundations of corporate risk posture, which are typically specified by standards like ISO 27001 or NIST. It implies that the organization's interaction with emerging technologies and the changing threat intelligence ecosystem affects risk posture, which is dynamic rather than static. Before to presently, risk models that divided risks and mitigation into two categories, for example, internal vs external, technical against human, need to be modified to take into account several factors. The incorporation of blockchain consensus mechanisms, IoT-enabled interface complexity, and AI-driven anomalies requires a new theoretical vocabulary to comprehend and categorize risk behavior.

5.3.2 Managerial Implications

For CEOs, IT directors, and cybersecurity specialists faced with negotiating the nexus of technical innovation and digital risk, the report has significant management implications. One of the most important lessons for managers is the necessity of making cybersecurity strategy a part of agendas for digital transformation. Cybersecurity is too frequently viewed as a back-end compliance issue, but our research shows that it has to be included in developing technology efforts from the very beginning. It is recommended that decision-

makers embrace proactive risk mapping that complements organizational capacity and technology innovation.

One particular consequence for managers is the implementation of frameworks for adaptive risk management that are sensitive to the quickly evolving hazards in cloud, IoT, and AI settings. According to the research, in situations where danger vectors may be created by machine learning algorithms or the interconnection of smart devices, static firewalls and general security rules are inadequate. Rather, managers need to support threat modelling techniques that leverage AI-powered forensic tools, real-time event detection, and behavioral analytics. These skills might aid security teams in anticipating risk situations based on new digital trends, in addition to identifying and eliminating attackers.

Lastly, the findings suggest that managers should take a decentralized approach to cybersecurity responsibilities inside the governance structure. Instead of consolidating risk management into one IT department, leadership ought to support cross-functional cybersecurity committees with members from customer relations, operations, finance, and law. This inclusive approach results in more sophisticated mitigation measures by placing risk inside each operational unit. These techniques also improve an organization's ability to respond to new risks and are consistent with agile management approaches.

5.4 Limitations of the Study

It is necessary to recognize several limitations to put the results in perspective and define the limits of their application, even with the rigorous methodological approach and analytical depth used in this work. Although the results are not invalidated by these limitations, they do offer important insight into the interpretive length and potential topics for further research.

Firstly, the sample period and participant profile are among the most important limitations. The majority of whom held management and mid-level technical positions, were selected from among professionals employed in cybersecurity or IT-related activities. Although it represents well-informed viewpoints, its composition could unintentionally leave out important perspectives from front-line operators, lower-level technical professionals, or non-technical stakeholders like the legal, compliance, and end-user groups. These viewpoints are important, especially when analyzing human-centric vulnerabilities that a technically oriented responder pool would miss, including social engineering, insider risks, or risk misperception.

Secondly, professionals in areas with competent digital infrastructures and legislative frameworks made up the majority of the respondents' geographic distribution. There may be

a geographical bias introduced, even while this guarantees familiarity with cutting-edge technologies like cloud computing, blockchain, IoT, and AI. Underrepresented are respondents from underdeveloped nations, where there are notable differences in cybersecurity knowledge, infrastructure, and policy enforcement. As a result, the results could not accurately represent organizational practices, risk perceptions, or resource limitations in middle- and low-income situations where governance structures and technology deployment may differ significantly.

Thirdly, one methodological limitation is that data were only collected using a standardized Likert-scale questionnaire. This method limited the depth of participant replies, even while it made standardized data gathering and statistical interpretation easier. Closed-ended questions were unable to capture nuanced insights, such as the reasoning behind particular risk perceptions, situational decision-making procedures, or interpretative variations in security maturity. For a more thorough investigation of the cognitive, organizational, and sociocultural elements affecting cybersecurity strategy and behavior, qualitative data, such as focus groups or open-ended interviews, would have been useful.

Subsequently, the survey also concentrated on five key technological areas: cloud computing, blockchain, IoT, AI, and 5G networks. Even though they are important for the cybersecurity environment today and in the future, newer areas like digital twins, augmented reality (AR), quantum computing, and bio-cyber systems were either completely ignored or just briefly discussed. If examined separately or over time, the risk vectors and mitigation strategies connected to these technologies may differ significantly and may have distinct theoretical or managerial ramifications.

another significant limitation is that cybersecurity risk evaluations are time-based. Because the threat landscape is changing so quickly, risk assessments and mitigation techniques are also subject to change. For example, they may drastically change when new vulnerabilities, legislative changes, or high-profile attacks occur. The study only documents one point in time; it excludes longitudinal tracking and scenario-based prediction, which might offer a more dynamic perspective of how cybersecurity status evolves with emerging technologies.

Lastly, the potential for response bias is increased by using self-reported data. Participants may misrepresent their company's cybersecurity maturity or underreport known vulnerabilities due to anticipated expectations or reputational concerns. Even in cases where

anonymity and secrecy were ensured, the inherent limitations of self-assessment instruments must be considered when evaluating the reliability of stated organizational practices.

5.5 Recommendations

5.5.1 For Improvements

Based on the findings of present study on cybersecurity risk in new technologies, several specific improvements are recommended for businesses, regulatory bodies, and technology developers in order to address existing vulnerabilities and fortify resilience frameworks.

First, companies utilizing advanced technologies such as blockchain, cloud computing, 5G, artificial intelligence, and the Internet of Things should prioritize cybersecurity integration throughout the design and implementation phases rather than viewing security to be a post-deployment patch. This entails implementing threat modelling frameworks (such as STRIDE or DREAD) and security-by-design concepts throughout the architectural phase. In particular, explainable AI (XAI) protocols should be implemented by AI-driven platforms to increase model openness and lower the risk of hostile manipulation. The implementation of device-level security protocols, such as firmware integrity verification, hardware root-of-trust mechanisms, and mutual authentication, is also necessary for IoT systems in order to guard against device-level attack.

Second, governance frameworks for cybersecurity need to be adjusted to reflect the ever-changing threat picture brought forth by developing technology. Companies could think about assigning specialized positions like "IoT Security Architects" or "AI Security Officers" to provide risk supervision that is vertically specific. Furthermore, internal cybersecurity policies need to change from general compliance checklists to flexible, risk-aware procedures that are regularly put to the test using simulated attack scenarios like adversarial penetration testing and red teaming. A regularly updated risk registry reflecting changing threat intelligence, especially that resulting from supply chain vulnerabilities or zero-day attacks, could support this adaptive governance strategy.

Third, every department should formalize capacity building and cross-functional cybersecurity training. This study demonstrates that non-technical teams' varying perceptions of cyber risk are one of the major risk drivers. The implementation of obligatory cybersecurity awareness programs that are specific to the departments of finance, operations, marketing, and development can help reduce human-centric vulnerabilities, including social engineering and misconfigurations. Additionally, companies want to use interactive training

dashboards and phishing simulation technologies that offer quantifiable results and behavior monitoring.

Fourth, data governance and automation of compliance are important areas for improvement, particularly in view of new privacy issues. It is crucial to incorporate privacy engineering strategies like homomorphic encryption, federated learning, and differential privacy when businesses gather enormous volumes of sensitive data via AI and IoT devices. These should be put into place not merely to comply with the CCPA or GDPR, but also to integrate ethical data management into the framework of operations. Additionally, regtech solutions that can dynamically analyze regulatory exposure, identify irregularities, and produce audit-ready data must be used to automate compliance monitoring.

Finally, there is a need to improve multi-stakeholder collaboration. Organizational silos cannot adequately handle cybersecurity in developing technologies. Governmental organizations, academic institutions, and industry consortia must actively collaborate on cyber-resilience. For instance, systems for exchanging threat intelligence between the public and commercial sectors, such as Information Sharing and Analysis Centers (ISACs), have to be expanded to include dangers unique to 5G, blockchain, and artificial intelligence. By providing real-time awareness of changing attack vectors and response tactics, this collective intelligence method would lower systemic risk throughout linked digital ecosystems.

5.5.2 For Future Research

Although this dissertation makes a substantial contribution to our understanding of cybersecurity threats related to new technologies, there are a few particular directions that demand more research in order to expand theoretical understanding and practical relevance.

First, especially in rapidly evolving fields like artificial intelligence and quantum computing, future research should use longitudinal approaches to monitor how cybersecurity risk perception and mitigation efficacy change over time. A time component would provide important information about how organizational plans, regulatory reactions, and risk appetite develop as technologies move from pilot stages to enterprise-wide adoption. A three-year longitudinal research on the effectiveness of AI model audits, for instance, may provide important information on adaptation curves and compliance fatigue.

Second, to comprehend how cultural, legal, and regional contexts impact cybersecurity risk practices in developing technologies, cross-cultural comparative studies have to be conducted. Only a fairly uniform sample of respondents, primarily from nations with

developed cyber policy ecosystems, was included in this study. Future studies should take into account viewpoints from poor nations, where differing threat environments, legislative frameworks, and resource constraints may lead to widely disparate approaches to cybersecurity governance and technology implementation.

Third, in order to examine multifaceted problems in developing technological settings, academics ought to pursue multidisciplinary techniques that integrate cybersecurity alongside behavioral science, ethics, and law. For example, executive decision-making about AI security investments may be significantly impacted by cognitive biases, and data governance procedures in cloud ecosystems may be influenced by ethical quandaries. To provide a more complete view of perceived and hidden cyber hazards, mixed-method approaches that combine quantitative risk assessment with qualitative empirical research or ethnographic techniques are needed.

Fourth, more detailed, domain-specific research is required to look more closely at cybersecurity frameworks for certain technologies. This study conducted a comprehensive evaluation of several technologies; however, in order to uncover specific dangers, compliance inconsistencies, and mitigation solutions, future research should concentrate solely on one area, like cybersecurity through smart contracts based on blockchain or AI-driven financial systems. In particular, research that examines deep fake identification systems in AI-powered media or tests the robustness of blockchain consensus systems under quantum risk models will fill important gaps in the body of literature.

Fifth, there is an urgent need for study on regulatory innovation and how it affects cybersecurity. Current legal frameworks are being challenged by emerging technologies, and little is known about how agile regulatory models, such algorithmic audit mandates or regulatory sandboxes, impact cybersecurity procedures. Future research should assess the effectiveness, difficulties in enforcing the law, and industry reaction to such innovative regulatory instruments, especially in critical infrastructure, healthcare, and finance.

Lastly, future studies have to look at modelling cyber resilience via digital twin and simulation technologies. Researchers should investigate the use of digital twin environments for stress-evaluating whole ecosystems against synchronized assaults, given the growing popularity of smart infrastructure and digital-physical systems. Particularly in vital industries such as energy, defence, and autonomous mobility, simulation-based research utilizing real-world sensors and threat intelligence data might greatly improve preparedness strategies.

6. References

Abikoye, B. E., Umeorah, S. C., Adelaja, A. O., Ayodele, O., & Ogunsuji, Y. M. (2024). Regulatory compliance and efficiency in financial technologies: Challenges and innovations. *World Journal of Advanced Research and Reviews*, *23*(1), 1830-1844.

Abir, S. A. A., Anwar, A., Choi, J., & Kayes, A. (2021). Iot-enabled smart energy grid: Applications and challenges. *IEEE access*, *9*, 50961-50

Acero, M. X., Minvielle, E., & Waelli, M. (2023). Understanding the activity of oncology nurse coordinators: An elaboration of a framework based on an abductive approach. *Health policy*, *130*, 104737.

Adeoye, M. A. (2023). Review of sampling techniques for education. *ASEAN Journal for Science Education*, *2*(2), 87-94.

Afaq, M., Shah, M., & Gul, N. (2023). The Role of Henchard's Character in Loss and Profit of His Business in the Novel the Mayor of Casterbridge. *Pakistan Languages and Humanities Review*, *7*(2), 318-327.

Ahmed, M. (Ed.). (2024). *Ransomware Evolution*. CRC Press.

Ahmed, S. K. (2024). How to choose a sampling technique and determine sample size for research: a simplified guide for researchers. *Oral Oncology Reports*, *12*, 100662.

Ahmed, S., Ahmed, I., Kamruzzaman, M., & Saha, R. (2022). Cybersecurity Challenges in IT Infrastructure and Data Management: A Comprehensive Review of Threats, Mitigation Strategies, and Future Trend. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *1*(01), 36-61.

Akmal, H. A. (2021). *Design by Play: Playfulness and Object-Oriented Philosophy for the design of IoT*. Lancaster University (United Kingdom).

Akpobome, O. (2024). The Impact of Emerging Technologies on Legal Frameworks: A Model for Adaptive Regulation. *International Journal of Research Publication and Reviews*, *5*(10), 5046-5060.

Al Rashdan, A. Y., Abdel-Khalik, H. S., Giraud, K. M., Cole, D. G., Farber, J. A., Clark, W. W., ... & Varuttamaseni, A. (2022). A qualitative strategy for fusion of physics into empirical models for process anomaly detection. *Energies*, *15*(15), 5640.

Alanazi, M. N. (2023). 5g security threat landscape, ai and blockchain. *Wireless Personal Communications*, *133*(3), 1467-1482.

Al-Dulaimy, A., Jansen, M., Johansson, B., Trivedi, A., Iosup, A., Ashjaei, M., ... & Papadopoulos, A. V. (2024). The computing continuum: From IoT to the cloud. *Internet of Things*, *27*, 101272.

Alfandi, O., Khanji, S., Ahmad, L., & Khattak, A. (2021). A survey on boosting IoT security and privacy through blockchain: Exploration, requirements, and open issues. *Cluster Computing*, *24*(1), 37-55.

Al-Farsi, S., Rathore, M. M., & Bakiras, S. (2021). Security of blockchain-based supply chain management systems: challenges and opportunities. *Applied Sciences*, *11*(12), 5585.

Alkhadra, R., Abuzaid, J., AlShammari, M., & Mohammad, N. (2021, July). Solar winds hack: In-depth analysis and countermeasures. In *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-7). IEEE.

Almazarqi, H. (2024). *Profiling IoT botnet activity* (Doctoral dissertation, University of Glasgow).

Almazarqi, H. (2024). *Profiling IoT botnet activity* (Doctoral dissertation, University of Glasgow).

Aloisi, A., & De Stefano, V. (2022). Essential jobs, remote work and digital surveillance: Addressing the COVID-19 pandemic panopticon. *International Labour Review*, *161*(2), 289-314.

Alwashali, A. A. M. A., Abd Rahman, N. A., & Ismail, N. (2021, December). A survey of ransomware as a service (RaaS) and methods to mitigate the attack. In *2021 14th International Conference on Developments in eSystems Engineering (DeSE)* (pp. 92-96). IEEE.

Alzoubaidi, A. R., Najdawi, A., & Alzoubaidi, M. (2023). Developing a Cybersecurity Risk Management Framework for Non-Technical Losses in National Power Distribution Companies. *Jordan Journal of Energy*, *1*(2).

Alzubaidi, L., Bai, J., Al-Sabaawi, A., Santamaría, J., Albahri, A. S., Al-Dabbagh, B. S. N., ... & Gu, Y. (2023). A survey on deep learning tools dealing with data scarcity: definitions, challenges, solutions, tips, and applications. *Journal of Big Data*, *10*(1), 46.

Amoo, O. O., Osasona, F., Atadoga, A., Ayinla, B. S., Farayola, O. A., & Abrahams, T. O. (2024). Cybersecurity threats in the age of IoT: A review of protective measures. *International Journal of Science and Research Archive*, *11*(1), 1304-1310.

AMRON, M. T. B. (2021). ACCEPTANCE AND READINESS MODEL OF CLOUD COMPUTING SERVICES FOR THE MALAYSIAN PUBLIC SECTORS PERSONNEL.

Anderson, L. (2021). *The Internet of Things: Security and Insecurity Challenges* (Master's thesis, Utica College).

Angel, N. A., Ravindran, D., Vincent, P. D. R., Srinivasan, K., & Hu, Y. C. (2021). Recent advances in evolving computing paradigms: Cloud, edge, and fog technologies. *Sensors*, *22*(1), 196.

Areo, G. (2024). Data-Driven Security in Healthcare: Ensuring the Integrity of Machine Learning Models for Aortic Stenosis Diagnosis.

Arora, R. K., Muqeem, M., & Saxena, M. (2024). Developing a Comprehensive Security Framework for Detecting and Mitigating IoT device Attack.

Ashogbon, A. D. (2021). *Examining the role of diffusion of innovation theory in cloud computing adoption: international marketing organization perspective*. Northcentral University.

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), 1333.

Attah, R. U., Garba, B. M. P., Gil-Ozoudeh, I., & Iwuanyanwu, O. (2024). Strategic frameworks for digital transformation across logistics and energy sectors: Bridging technology with business strategy. *Open Access Res J Sci Technol*, *12*(02), 070-80.

Augustine, N., Sultan, A. B. M., Osman, M. H., & Sharif, K. Y. (2024). Application of Artificial Intelligence in Detecting SQL Injection Attacks. *JOIV: International Journal on Informatics Visualization*, *8*(4), 2131-2138.

Bansal, A., Kapil, D., Anupriya, S. A., & Gupta, V. K. (2022). Analysis and Detection of various DDoS attacks on Internet of Things Network. *International Journal of Wireless and Microwave Technologies*, *12*(3), 18-32.

Barlybayev, A., Sharipbay, A., Shakhmetova, G., & Zhumadillayeva, A. (2024). Development of a Flexible Information Security Risk Model Using Machine Learning Methods and Ontologies. *Applied Sciences*, *14*(21), 9858.

Baseri, Y., Chouhan, V., & Ghorbani, A. (2024). Cybersecurity in the quantum era: Assessing the impact of quantum computing on infrastructure. *arXiv preprint arXiv:2404.10659*.

Baviskar, C. R. (2022). *Cloud based automated encryption approach to prevent S3 bucket leakage using AWS Lambda* (Doctoral dissertation, Dublin, National College of Ireland).

Bergmann, J. (2023). Research philosophy, methodological implications, and research design. In *At Risk of Deprivation: The Multidimensional Well-Being Impacts of Climate Migration and Immobility in Peru* (pp. 57-89). Wiesbaden: Springer Fachmedien Wiesbaden.

Beshley, M., Klymash, M., Scherm, I., Beshley, H., & Shkoropad, Y. (2022, February). Emerging network technologies for digital transformation: 5G/6G, IoT, SDN/IBN, cloud computing, and blockchain. In *IEEE lnternational Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering* (pp. 1-20). Cham: Springer Nature Switzerland.

Bhushan, B., Sinha, P., & Sagayam, K. M. (2021). Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. *Computers & Electrical Engineering*, *90*, 106897.

Bhutani, A., & Sanaria, A. (2023). The past, present and future in artificial intelligence. *GLMS J Manag Rev Transform*, *2*, 132-140.

Bofill, M., Coll, J., Martín, G., Suy, J., & Villaret, M. (2022). The sample analysis machine scheduling problem: Definition and comparison of exact solving approaches. *Computers & Operations Research*, *142*, 105730.

Bragazzi, N. L., Kong, J. D., Mahroum, N., Tsigalou, C., Khamisy-Farah, R., Converti, M., & Wu, J. (2023). Epidemiological trends and clinical features of the ongoing monkeypox epidemic: a preliminary pooled data analysis and literature review. *Journal of medical virology*, *95*(1), e27931.

Branley-Bell, D., Coventry, L., Dixon, M., Joinson, A. and Briggs, P., 2022. Exploring age and gender differences in ICT cybersecurity behaviour. *Human Behavior and Emerging Technologies*, *2022*(1), p.2693080.

Brezavšček, A., & Baggia, A. (2025). Recent Trends in Information and Cyber Security Maturity Assessment: A Systematic Literature Review. *Systems*, *13*(1), 52.

Burita, L., & Le, D. T. (2021, October). Cyber security and APT groups. In *2021 Communication and Information Technologies (KIT)* (pp. 1-7). IEEE.

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. *Risk Analysis*, *42*(8), 1643-1669.

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. *Risk Analysis*, *42*(8), 1643-1669.

Chauhan, D., Ahmad, H. S., Subtirelu, R., Mannam, S., Turlip, R., Bryan, K., ... & Yoon, J. W. (2023). Defining the minimal clinically important difference in smartphone-based mobility after spine surgery: correlation of survey questionnaire to mobility data: presented at the 2023 AANS/CNS joint section on disorders of the spine and peripheral nerves. *Journal of Neurosurgery: Spine*, *39*(3), 427-437.

Cheron, C., Salvagni, J., & Colomby, R. K. (2022). The qualitative approach interview in administration: A guide for researchers. *Revista de Administração Contemporânea*, *26*, e210011.

Chervenak, F. A., & McCullough, L. B. (2021). Ethical considerations. In *Clinical Maternal-Fetal Medicine* (pp. 42-1). CRC Press.

Chiara, P. G. (2022). The IoT and the new EU cybersecurity regulatory landscape. *International Review of Law, Computers & Technology*, *36*(2), 118-137.

Cordey, S. (2023). *Software supply chain attacks: An illustrated typological review*. ETH Zurich.

Csenkey, K., & Bindel, N. (2023). Post-quantum cryptographic assemblages and the governance of the quantum threat. *Journal of Cybersecurity*, *9*(1), tyad001.

Dalal, Y. M., Supreeth, S., Amuthabala, K., Satheesha, T. Y., Asha, P. N., & Somanath, S. (2024, September). Optimizing Security: A Comparative Analysis of RSA, ECC, and DH Algorithms. In *2024 IEEE North Karnataka Subsection Flagship International Conference (NKCon)* (pp. 1-6). IEEE.

Daulatkar, S., & Deore, A. (2022, March). Post Covid-19 sentiment analysis of success of online learning: A case study of India. In *2022 9th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 460-465). IEEE.

Dave, T., Athaluri, S. A., & Singh, S. (2023). ChatGPT in medicine: an overview of its applications, advantages, limitations, future prospects, and ethical considerations. *Frontiers in artificial intelligence*, *6*, 1169595.

Davies, T. (2022). A review of topological data analysis for cybersecurity. *arXiv preprint arXiv:2202.08037*.

De Fina, A. (2021). Doing narrative analysis from a narratives-as-practices perspective. *Narrative Inquiry*, *31*(1), 49-71.

Decker, N. (2025). The Economic Bomb: A Strategic Financial Warfare Tactic.

Desidera, S., Chauvin, G., Bonavita, M., Messina, S., LeCoroller, H., Schmidt, T. O. B. I. A. S., ... & Wildi, F. (2021). The SPHERE infrared survey for exoplanets (SHINE)-I. Sample definition and target characterization. *Astronomy & Astrophysics*, *651*, A70.

Dey, T. K., & Wang, Y. (2022). *Computational topology for data analysis*. Cambridge University Press.

Dhayanidhi, G. (2022). Research on IoT threats & implementation of AI/ML to address emerging cybersecurity issues in IoT with cloud computing.

Di Federico, G., & Barcaroli, F. (2022). *Cloud Identity Patterns and Strategies: Design enterprise cloud identity models with OAuth 2.0 and Azure Active Directory*. Packt Publishing Ltd.

Diller, S. J., & Passmore, J. (2023). Defining digital coaching: a qualitative inductive approach. *Frontiers in Psychology*, *14*, 1148243.

Duque, J., Godinho, A., & Vasconcelos, J. (2022). Knowledge data extraction for business intelligence A design science research approach. *Procedia Computer Science*, *204*, 131-139.

Dwivedi, K., Agrawal, A., Bhatia, A., & Tiwari, K. (2024). A novel classification of attacks on blockchain layers: Vulnerabilities, attacks, mitigations, and research directions. *arXiv preprint arXiv:2404.18090*.

Ebot, A. (2024). *Technology Acceptance Model for Adopting Cybersecurity Technology in Small and Medium Business/Enterprise: A Generic Qualitative Study* (Doctoral dissertation, Capella University).

Edwards, D. J. (2024). Inventory and Control of Enterprise (Hardware) Assets. In *Critical Security Controls for Effective Cyber Defense: A Comprehensive Guide to CIS 18 Controls* (pp. 1-28). Berkeley, CA: Apress.

El Husseini, F., Noura, H., Salman, O., & Chehab, A. (2024, December). Advanced Machine Learning Approaches for Zero-Day Attack Detection: A Review. In *2024 8th Cyber Security in Networking Conference (CSNet)* (pp. 297-304). IEEE.

Erinle, Y., Kethepalli, Y., Feng, Y., & Xu, J. (2023). Sok: Design, vulnerabilities, and security measures of cryptocurrency wallets. *arXiv preprint arXiv:2307.12874*.

Fakhouri, H. N., Alawadi, S., Awaysheh, F. M., Hani, I. B., Alkhalaileh, M., & Hamad, F. (2023). A comprehensive study on the role of machine learning in 5G security: Challenges, technologies, and solutions. *Electronics*, *12*(22), 4604.

Fakir, J. (2024). *An investigation of cybersecurity implementation challenges among South African SMEs* (Master's thesis, University of the Witwatersrand, Johannesburg (South Africa)).

Faklaris, C. (2022). *Toward a Socio-Cognitive Stage Model of Cybersecurity Behavior Adoption* (Doctoral dissertation, US National Science Foundation).

Fallatah, W., Kävrestad, J., & Furnell, S. (2024). Establishing a Model for the User Acceptance of Cybersecurity Training. *Future Internet*, *16*(8), 294.

Faturahman, A., Agarwal, V., & Lukita, C. (2021). Blockchain technology-the use of cryptocurrencies in digital revolution. *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, *3*(1), 53-59.

Filipenko, N., Lukashevych, S., Andrieieva, O., & Ivanović, A. (2024). Application of artificial intelligence and information and communication technologies: Socio-ethical problems. *Theory and Practice of Forensic Science and Criminalistics*, *34*(1), 12-41.

Folorunso, A., Mohammed, V., Wada, I., & Samuel, B. (2024). The impact of ISO security standards on enhancing cybersecurity posture in organizations. *World Journal of Advanced Research and Reviews*, *24*(1), 2582-2595.

Futane, A. G., & Tech, B. (2021). 24. Sampling Technique in Research Methodology. *CONTEMPORARY MULTI-DISCIPLINARY RESEARCH TREND*, 228.

Gamage, A. N. (2025). Research Design, Philosophy, and Quantitative Approaches in Scientific Research Methodology. *Sch J Eng Tech*, *2*, 91-103.

George, A. S., & George, A. H. (2024). Riding the wave: an exploration of emerging technologies reshaping modern industry. *Partners Universal International Innovation Journal*, *2*(1), 15-38.

George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. *Partners Universal International Innovation Journal*, *2*(1), 51-75.

Goldblum, M., Tsipras, D., Xie, C., Chen, X., Schwarzschild, A., Song, D., ... & Goldstein, T. (2022). Dataset security for machine learning: Data poisoning, backdoor attacks, and defenses. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *45*(2), 1563-1580.

Golzar, J., Noor, S., & Tajik, O. (2022). Convenience sampling. *International Journal of Education & Language Studies*, *1*(2), 72-77.

Goni, A., Jahangir, M. U. F., & Chowdhury, R. R. (2024). A study on cyber security: Analyzing current threats, navigating complexities, and implementing prevention

strategies. *International Journal of Research and Scientific Innovation*, *10*(12), 507-522.

Goudarzi, A., Ghayoor, F., Waseem, M., Fahad, S., & Traore, I. (2022). A survey on IoT-enabled smart grids: emerging, applications, challenges, and outlook. *Energies*, *15*(19), 6984.

Gündüz, M. Z., & Daş, R. (2025). Smart grid: Interoperability and cyber security. In *Cyber Security Solutions for Protecting and Building the Future Smart Grid* (pp. 299-320). Elsevier.

Guo, F., Susilo, W., Chen, X., Jiang, P., Lai, J., & Zhao, Z. (2023). Research Philosophy of Modern Cryptography. *IACR Cryptol. ePrint Arch.*, *2023*, 715.

Hall, J. R., Savas-Hall, S., & Shaw, E. H. (2023). A deductive approach to a systematic review of entrepreneurship literature. *Management Review Quarterly*, *73*(3), 987-1016.

Hasan, N., Rana, R. U., Chowdhury, S., Dola, A. J., & Rony, M. K. K. (2021). Ethical considerations in research. *Journal of Nursing Research, Patient Safety and Practise (JNRPSP) 2799-1210*, *1*(01), 1-4.

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business & Economics*, *3*(5), 97.

HIZA, D. (2022). *Assessig the Significance of Cia Triad Security Model in Establishing ICT Security Controls in The Public Sector* (Doctoral dissertation, Institute of Accountancy Arusha (IAA)).

Hoda, R. (2024). Research Philosophy. In *Qualitative Research with Socio-Technical Grounded Theory: A Practical Guide to Qualitative Data Analysis and Theory Development in the Digital World* (pp. 93-112). Cham: Springer International Publishing.

Hurley, E., Dietrich, T., & Rundle-Thiele, S. (2021). Integrating theory in co-design: An abductive approach. *Australasian Marketing Journal*, *29*(1), 66-77.

Hwang, G. J., & Chien, S. Y. (2022). Definition, roles, and potential research issues of the metaverse in education: An artificial intelligence perspective. *Computers and Education: Artificial Intelligence*, *3*, 100082.

Islam, M. T., Munir, A. B., & Karim, M. E. (2021). Revisiting the right to privacy in the digital age: A quest to strengthen the Malaysian data protection regime. *JMCL*, *48*, 49.

Jimmy, F. (2021). Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. *Valley International Journal Digital Library*, *1*, 564-74.

Jimmy, F. (2021). Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. *Valley International Journal Digital Library*, *1*, 564-74.

Kaddoura, S., & Al Husseiny, F. (2023). The rising trend of Metaverse in education: Challenges, opportunities, and ethical considerations. *PeerJ Computer Science*, *9*, e1252.

Kalinin, M., Krundyshev, V., & Zegzhda, P. (2021). Cybersecurity risk assessment in smart city infrastructures. *Machines*, *9*(4), 78.

Kanwal, K., Shi, W., Kontovas, C., Yang, Z., & Chang, C. H. (2024). Maritime cybersecurity: are onboard systems ready?. *Maritime Policy & Management*, *51*(3), 484-502.

Khan, R., Taqi, M., & Afzal, A. (2024). Deepfakes in Finance: Unraveling the Threat Landscape and Detection Challenges. In *Navigating the World of Deepfake Technology* (pp. 91-120). IGI Global.

Khan, S., Kabanov, I., Hua, Y., & Madnick, S. (2022). A systematic analysis of the capital one data breach: Critical lessons learned. *ACM Transactions on Privacy and Security*, *26*(1), 1-29.

Khanna, A. (2025). Introduction to Cybersecurity. In *Securing an Enterprise: Maximizing Digital Experiences through Enhanced Security Measures* (pp. 3-18). Berkeley, CA: Apress.

Kiani, A. K., Pheby, D., Henehan, G., Brown, R., Sieving, P., Sykora, P., ... & International Bioethics Study Group. (2022). Ethical considerations regarding animal experimentation. *Journal of preventive medicine and hygiene*, *63*(2 Suppl 3), E255.

Knapp, E. D. (2024). *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Elsevier.

Kosutic, D., & Pigni, F. (2022). Cybersecurity: investing for competitive outcomes. *Journal of Business Strategy*, *43*(1), 28-36.

Krasner, H. (2021). The cost of poor software quality in the US: A 2020 report. *Proc. Consortium Inf. Softw. QualityTM (CISQTM)*, *2*, 3.

Krishnamoorthy, S., Dua, A., & Gupta, S. (2023). Role of emerging technologies in future IoT-driven Healthcare 4.0 technologies: A survey, current challenges and future directions. *Journal of Ambient Intelligence and Humanized Computing*, *14*(1), 361-407.

Kudzko, A., & Burilkov, A. (2025). Private Tech for Resilience: Geopolitical Shifts and Government-Tech Relations.

Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. *Neural Computing and Applications*, *34*(18), 15241-15271.

Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. *Neural Computing and Applications*, *34*(18), 15241-15271.

Lakshmi, D., & Tyagi, A. K. (Eds.). (2024). Emerging Technologies and Security in Cloud Computing.

Lameijer, B. A., Pereira, W., & Antony, J. (2021). The implementation of Lean Six Sigma for operational excellence in digital emerging technology companies. *Journal of manufacturing technology management*, *32*(9), 260-284.

Landoll, D. (2021). *The security risk assessment handbook: A complete guide for performing security risk assessments*. CRC press.

Latino, M. E., & Menegoli, M. (2022). Cybersecurity in the food and beverage industry: A reference framework. *Computers in Industry*, *141*, 103702.

Lavarda, R., & Bellucci, C. F. (2022). Case study as a suitable method to research strategy as practice perspective. *The Qualitative Report*, *27*(2), 539-555.

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659-671.

Lehto, M. (2022). Cyber-attacks against critical infrastructure. In *Cyber security: Critical infrastructure protection* (pp. 3-42). Cham: Springer International Publishing.

Lewallen, J. (2021). Emerging technologies and problem definition uncertainty: The case of cybersecurity. *Regulation & governance*, *15*(4), 1035-1052.

Li, K., Wang, Z., Wang, Y., Luo, B., & Li, F. (2023, November). Poster: ethics of computer security and privacy research-trends and standards from a data perspective. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (pp. 3558-3560).

Liu, P., & Lu, C. (2021). Strategic analysis and development plan design on digital transformation in the energy industry: A global perspective. *International Journal of Energy Research*, *45*(14), 19657-19670.

Lyu, M., Farooq, J., & Zhu, Q. (2024). Mapping Cyber Threats in the 5G Supply Chain: Landscape, Vulnerabilities, and Risk Management. *IEEE Network*.

Mahmood, S., Chadhar, M., & Firmin, S. (2022). Cybersecurity challenges in blockchain technology: A scoping review. *Human Behavior and Emerging Technologies*, *2022*(1), 7384000.

Malik, M. A. A., Mustapha, M. F., Sobri, N. M., Abd Razak, N. F., Zaidi, M. N. M., Shukri, A. A., & Sham, M. A. L. Z. (2021). Optimal reliability and validity of measurement model in confirmatory factor analysis: different likert point scale experiment. *Journal of Contemporary Issues and Thought*, *11*, 105-112.

Mamatha, G. S., Dimri, N., & Sinha, R. (2024). Post-Quantum Cryptography: Securing Digital Communication in the Quantum Era. *arXiv preprint arXiv:2403.11741*.

Mancuso, J. (2023). *Motives and Tactics, Techniques, and Procedures: Making Sense of the Activities of Russian Advanced Persistent Threat Groups*. Utica University.

Manjarres, M. P., & Zwierewicz, M. (2021). Pedagogical practice, metacognition, and reading comprehension in a foreign language: a systematic review from a deductive approach. *Educação e Pesquisa*, *47*.

Maurer, T., & Morgus, R. (2022). *Compilation of existing cybersecurity and information security related definitions*. New America.

Mazhar, S. A., Anjum, R., Anwar, A. I., & Khan, A. A. (2021). Methods of data collection: A fundamental tool of research. *Journal of Integrated Community Health*, *10*(1), 6-10.

Mbanaso, U. M., Abrahams, L., & Okafor, K. C. (2023). Research philosophy, design and methodology. In *Research Techniques for Computer Science, Information Systems and Cybersecurity* (pp. 81-113).

Meeker, W. Q., Escobar, L. A., & Pascual, F. G. (2021). *Statistical methods for reliability data*. John Wiley & Sons.

Mekala, S. H., Baig, Z., Anwar, A., & Zeadally, S. (2023). Cybersecurity for Industrial IoT (IIoT): Threats, countermeasures, challenges and future directions. *Computer Communications*, *208*, 294-320.

Mesiä, M. (2024). Nationwide vulnerability coordination.

Mezzanotte, P., Palazzi, V., Alimenti, F., & Roselli, L. (2021). Innovative RFID sensors for Internet of Things applications. *IEEE Journal of Microwaves*, *1*(1), 55-65.

Milousi, K., Kiriakidis, P., Mengidis, N., Rizos, G., Mazi, M. S., Voulgaridis, A., ... & Tzovaras, D. (2024, July). Evaluating Cybersecurity Risk: A Comprehensive Comparison of Vulnerability Scoring Methodologies. In *Proceedings of the 19th International Conference on Availability, Reliability and Security* (pp. 1-11).

Mithas, S., Chen, Z. L., Saldanha, T. J., & De Oliveira Silveira, A. (2022). How will artificial intelligence and Industry 4.0 emerging technologies transform operations management?. *Production and Operations Management*, *31*(12), 4475-4487.

Mızrak, F. (2023). Integrating cybersecurity risk management into strategic management: a comprehensive literature review. *Research Journal of Business and Management*, *10*(3), 98-108.

Mızrak, F. (2023). Integrating cybersecurity risk management into strategic management: a comprehensive literature review. *Research Journal of Business and Management*, *10*(3), 98-108.

Mohamad, A. R. B., Yaakop, M. R., & Razif, M. A. B. M. (2024). The efficacy of the Malaysian Government's response towards cybercrime. *Open Journal of Political Science*, *14*(1), 166-176.

Möller, D. P. (2023). Cybersecurity in digital transformation. In *Guide to cybersecurity in digital transformation: Trends, methods, technologies, applications and best practices* (pp. 1-70). Cham: Springer Nature Switzerland.

Möller, D. P. (2023). NIST cybersecurity framework and MITRE cybersecurity criteria. In *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices* (pp. 231-271). Cham: Springer Nature Switzerland.

Möller, D. P. (2023). Ransomware attacks and scenarios: Cost factors and loss of reputation. In *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices* (pp. 273-303). Cham: Springer Nature Switzerland.

Mottron, L. (2021). A radical change in our autism research strategy is needed: Back to prototypes. *Autism research*, *14*(10), 2213-2220.

Mtisi, S. (2022). The qualitative case study research strategy as applied on a rural enterprise development doctoral research project. *International Journal of Qualitative Methods*, *21*, 16094069221145849.

Muir, A., Brown, K., & Girma, A. (2024, November). Reviewing the Effectiveness of Multi-factor Authentication (MFA) Methods in Preventing Phishing Attacks. In *Proceedings of the Future Technologies Conference* (pp. 597-607). Cham: Springer Nature Switzerland.

Murino, G., Ribaudo, M., Romano, S. P., Tacchella, A., Armando, A., & Colajanni, M. (2021, June). OT Cyber Security Frameworks Comparison Tool (CSFCTool). In *ITASEC* (pp. 9-22).

Naseem, M. L. (2024). Trans-IFFT-FGSM: a novel fast gradient sign method for adversarial attacks. *Multimedia Tools and Applications*, *83*(29), 72279-72299.

Negnevitsky, M. (2024). The History Of Artificial Intelligence Or From The. *WIT Transactions on Information and Communication Technologies*, *19*.

Ning, R., Bu, W., Yang, J., & Duan, S. (2023, August). A survey of detection methods research on living-off-the-land techniques. In *2023 IEEE International Conference on Sensors, Electronics and Computer Engineering (ICSECE)* (pp. 159-164). IEEE.

Nookala, G., Gade, K. R., Dulam, N., & Thumburu, S. K. R. (2024). Post-quantum cryptography: Preparing for a new era of data encryption.

Okafor, C. M., Kolade, A., Onunka, T., Daraojimba, C., Eyo-Udo, N. L., Onunka, O., & Omotosho, A. (2023). Mitigating cybersecurity risks in the US healthcare sector. *International Journal of Research and Scientific Innovation (IJRSI)*, *10*(9), 177-193.

Olaiya, O. P., Adesoga, T. O., Ojo, A., Olagunju, O. D., Ajayi, O. O., & Adebayo, Y. O. (2024). Cybersecurity strategies in fintech: safeguarding financial data and assets. *GSC Advanced Research and Reviews*, *20*(1), 50-56.

Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies applicatio. *World Journal of Advanced Research and Reviews*, *21*(3), 625-643.

Packard, N. (2023). Internet prehistory: ARPANET chronology. *Cogent Social Sciences*, *9*(2), 2245237.

Piszcz, A., Rojek, I., & Mikołajewski, D. (2024). Impact of Virtual Reality on Brain–Computer Interface Performance in IoT Control—Review of Current State of Knowledge. *Applied Sciences*, *14*(22), 10541.

Qian, X. (2024). Redefining International Law Paradigms: Charting Cybersecurity, Trade, and Investment Trajectories within Global Legal Boundaries. *The Journal of World Investment & Trade*, *25*(3), 295-333.

Qudus, L. (2025). Advancing cybersecurity: strategies for mitigating threats in evolving digital and IoT ecosystems. *Int Res J Mod Eng Technol Sci*, *7*(1), 3185.

Qudus, L. (2025). Cybersecurity governance: Strengthening policy frameworks to address global cybercrime and data privacy challenges.

Radanliev, P. (2023). Cyber-attacks on Public Key Cryptography. *Preprint*.

Rahman, M. M., Tabash, M. I., Salamzadeh, A., Abduli, S., & Rahaman, M. S. (2022). Sampling techniques (probability) for quantitative social science researchers: a conceptual guidelines with examples. *Seeu Review*, *17*(1), 42-51.

Rahman, T. (2025). The US Approach to Cybersecurity in the Energy Sector. In *The Palgrave Handbook of Cybersecurity, Technologies and Energy Transitions* (pp. 1-52). Cham: Springer Nature Switzerland.

Rai, D. H. (2024). Artificial Intelligence Through Time: A Comprehensive Historical Review.

Rascão, J. (2024). Reflection on Human Intelligence vs Artificial Intelligence and the Digital Society (from Theory to Practice). *American Journal of Humanities and Social Sciences Research (AJHSSR)*.

Rathore, R. S., Hewage, C., Kaiwartya, O., & Lloret, J. (2022). In-vehicle communication cyber security: challenges and solutions. *Sensors*, *22*(17), 6679.

Razdan, S., & Sharma, S. (2022). Internet of medical things (IoMT): Overview, emerging technologies, and case studies. *IETE technical review*, *39*(4), 775-788.

Razikin, K., & Soewito, B. (2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. *Egyptian Informatics Journal*, *23*(3), 383-404.

Rojas, R. V. B. (2024). Artificial Intelligence: Genesis, Development, and Future. In *Revolutionizing Communication* (pp. 1-15). CRC Press.

Saalbach, K. P. (2024). Attribution of Cyber Attacks. In *Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace* (pp. 251-275). Wiesbaden: Springer Fachmedien Wiesbaden.

Sabharwal, R., & Miah, S. J. (2022). An intelligent literature review: adopting inductive approach to define machine learning applications in the clinical domain. *Journal of Big Data*, *9*(1), 53.

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, *23*(15), 6666.

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, *23*(15), 6666.

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, *15*(18), 13369.

Salmona, M., & Kaczynski, D. (2024). Qualitative data analysis strategies. In *How to conduct qualitative research in finance* (pp. 80-96). Edward Elgar Publishing.

Sandiford, P. J., & Schührer, S. (2025). A negotiated/personal perspective and overview of research philosophy. In *Exploring Research Methodology and Research Design* (pp. 10-19). Edward Elgar Publishing.

Sania, N. S., Gigras, Y., & Mahajan, S. (2024). Gatividhi Guard: The Activity Guardian—Revolutionizing Security Information and Event Management (SIEM) Technology. *Journal of Operating Systems Development & Trends*, *11*(1), 29-44p.

Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. *SN computer science*, *2*(3), 160.

Sarker, I. H. (2024). *AI-driven cybersecurity and threat intelligence: cyber automation, intelligent decision-making and explainability*. Springer Nature.

Sarker, M., & AL-Muaalemi, M. A. (2022). Sampling techniques for quantitative research. In *Principles of social research methodology* (pp. 221-234). Singapore: Springer Nature Singapore.

Scharfman, J. (2024). Decentralized autonomous organization (dao) fraud, hacks, and controversies. In *The Cryptocurrency and Digital Asset Fraud Casebook, Volume II: DeFi, NFTs, DAOs, Meme Coins, and Other Digital Asset Hacks* (pp. 65-106). Cham: Springer Nature Switzerland.

Schiliro, F. (2023). Towards a contemporary definition of cybersecurity. *arXiv preprint arXiv:2302.02274*.

Schnitzer, S., & Tiruwuha, M. H. (2024). Transparency in the Black Box.

Schrum, M., Ghuy, M., Hedlund-Botti, E., Natarajan, M., Johnson, M., & Gombolay, M. (2023). Concerning trends in likert scale usage in human-robot interaction: Towards improving best practices. *ACM Transactions on Human-Robot Interaction*, *12*(3), 1-32.

Shafiq, M., Gu, Z., Cheikhrouhou, O., Alhakami, W., & Hamam, H. (2022). The Rise of "Internet of Things": Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks. *Wireless Communications and Mobile Computing*, *2022*(1), 8669348.

Shah, H., Shah, D., Jadav, N. K., Gupta, R., Tanwar, S., Alfarraj, O., ... & Marina, V. (2023). Deep learning-based malicious smart contract and intrusion detection system for IoT environment. *Mathematics*, *11*(2), 418.

Shakeel, S., Solangi, S. A., Fatima, U., & Nazir, N. (2023). THE STUDY OF EXISTENTIALISM IN ELIF SHAFAK'S NOVEL '10 MINUTES 38 SECONDS IN THIS STRANGE WORLD'THROUGH THE CHARACTER OF LEILA. *Harf-o-Sukhan*, *7*(4), 71-76.

Shemakov, R. (2025). *Centralized: Notes on Hydraulic and Digital Infrastructure*. Springer Nature.

Siddique, I. (2022). Balancing Innovation and Regulation: Requirements Engineering for Emerging Technologies. *European Journal of Advances in Engineering and Technology*, *9*(11), 95-99.

Singh, A. J., & Singh, A. P. (2024). Evolution of Information Technology: A Comprehensive Review. *Asian Journal of Current Research*, *9*(4), 78-90.

Sipponen, T. (2022). Information Security Testing Plan Model for Secure Software Development.

Soon, V. R. H., & Cooray, M. (2021). Surveillance Technology and Cultural Notions of Privacy: Development of the Laws in Malaysia. *The Malayan Journal clxix*.

Staines, L., Healy, C., Coughlan, H., Clarke, M., Kelleher, I., Cotter, D., & Cannon, M. (2022). Psychotic experiences in the general population, a review; definition, risk factors, outcomes and interventions. *Psychological Medicine*, *52*(15), 3297-3308.

Steingartner, W., Galinec, D., & Kozina, A. (2021). Threat defense: Cyber deception approach and education for resilience in hybrid threats model. *Symmetry*, *13*(4), 597.

Taherdoost, H. (2022). Cybersecurity vs. information security. *Procedia Computer Science*, *215*, 483-487.

Tanikonda, A., Pandey, B. K., Peddinti, S. R., & Katragadda, S. R. (2022). Advanced AI-Driven Cybersecurity Solutions for Proactive Threat Detection and Response in Complex Ecosystems. *Journal of Science & Technology*, *3*(1).

Tarlaci, S. (2022). *NeuroQuantology: quantum physics in brain: reducing the secret of the rainbow to the colours of a prism*. SULTAN TARLACI.

Temitope Olayinka, O. (2025). Built for Speed, Breached by Threats: The Cybersecurity Dilemma of Digital Transformation. *International Journal of Innovative Science and Research Technology*, *10*(4), 1963-1967.

Teuguia, F. (2025). Navigating the Legal Landscape of APIs: Innovations, Strategies for Sustainable, Inclusive, and Secure Digital Ecosystems. *World Futures*, 1-36.

Thach, N. N., Hanh, H. T., Huy, D. T. N., Nga, L. T. V., Huong, L. T. T., & Vu, Q. N. (2021). technology quality management of the industry 4.0 and cybersecurity risk management on current banking activities in emerging markets-the case in Vietnam. *International Journal for Quality Research*, *15*(3), 845.

Thach, N. N., Hanh, H. T., Huy, D. T. N., Nga, L. T. V., Huong, L. T. T., & Vu, Q. N. (2021). technology quality management of the industry 4.0 and cybersecurity risk management on current banking activities in emerging markets-the case in Vietnam. *International Journal for Quality Research*, *15*(3), 845.

Toheeb, O. A., Daniel, J., & Jackson, D. (2025). Smart Contracts and Automated Network Management.

Tsai, C. C., Lin, C. C., & Liao, S. W. (2023, December). Unveiling Vulnerabilities in DAO: A Comprehensive Security Analysis and Protective Framework. In *2023 IEEE International Conference on Blockchain (Blockchain)* (pp. 151-158). IEEE.

Tusher, H. M., Munim, Z. H., Notteboom, T. E., Kim, T. E., & Nazir, S. (2022). Cyber security risk assessment in autonomous shipping. *Maritime economics & logistics*, *24*(2), 208-227.

Umoga, U. J., Sodiya, E. O., Amoo, O. O., & Atadoga, A. (2024). A critical review of emerging cybersecurity threats in financial technologies. *International Journal of Science and Research Archive*, *11*(1), 1810-1817.

Utinková, H. (2021). Cyber Attacks against Iran as Instruments of Hybrid Warfare.

van Assen, M., Muscogiuri, E., Tessarin, G., & De Cecco, C. N. (2022). Artificial intelligence: A century-old story. In *Artificial Intelligence in Cardiothoracic Imaging* (pp. 3-13). Cham: Springer International Publishing.

Van Haute, E. (2021). Sampling techniques. *Research Methods in the Social Sciences: An AZ of Key Concepts; Oxford University Press: Oxford, UK*, 247.

Vogel, T. P., Top, K. A., Karatzios, C., Hilmers, D. C., Tapia, L. I., Moceri, P., ... & Munoz, F. M. (2021). Multisystem inflammatory syndrome in children and adults (MIS-C/A): Case definition & guidelines for data collection, analysis, and presentation of immunization safety data. *Vaccine*, *39*(22), 3037-3049.

Vsevolozhsky, G., & Qu, Y. (2022, December). A Process Model for Ensuring Diffusion and Adhesion of Cybersecurity Innovations in Software Development Organizations. In *2022 International Conference on Computational Science and Computational Intelligence (CSCI)* (pp. 1872-1878). IEEE.

Wan, Y., Qu, Y., Ni, W., Xiang, Y., Gao, L., & Hossain, E. (2024). Data and model poisoning backdoor attacks on wireless federated learning, and the defense mechanisms: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, *26*(3), 1861-1897.

Wang, C., Liu, S., Yang, H., Guo, J., Wu, Y., & Liu, J. (2023). Ethical considerations of using ChatGPT in health care. *Journal of Medical Internet Research*, *25*, e48009.

Watson, D. T. (2022). Malware Detection and Prevention.

Weiss, C. R., & Johnson-Koenke, R. (2023). Narrative inquiry as a caring and relational research approach: Adopting an evolving paradigm. *Qualitative Health Research*, *33*(5), 388-399.

West, M., Al-Douri, A., Hartmann, K., Buttner, W., & Groth, K. M. (2022). Critical review and analysis of hydrogen safety data collection tools. *International Journal of Hydrogen Energy*, *47*(40), 17845-17858.

Williams, T. L. (2021). *Cybersecurity: Zero-day vulnerabilities and attack vectors* (Doctoral dissertation, Northcentral University).

Wulf, F., Lindner, T., Strahringer, S., & Westner, M. (2021). IaaS, PaaS, or SaaS? The why of cloud computing delivery model selection: Vignettes on the post-adoption of cloud computing. In *Proceedings of the 54th Hawaii International Conference on System Sciences, 2021* (pp. 6285-6294).

Wynn, M., & Bechkoum, K. (2024). Emerging Technologies, Sustainable Engineering and Cybersecurity in the Digital Age. *Sustainability*, *16*(17), 7364.

Yaseen, A. (2024). Enhancing Cybersecurity through Automated Infrastructure Management: A Comprehensive Study on Optimizing Security Measures. *Quarterly Journal of Emerging Technologies and Innovations*, *9*(1), 38-60.

Yerlikaya, F. A., & Bahtiyar, Ş. (2022). Data poisoning attacks against machine learning algorithms. *Expert Systems with Applications*, *208*, 118101.

Yujia, F., Changhai, T., Xiaohuang, L., Xingli, S., Zemin, Y., & Yiwen, Z. (2022). Definition, classification, observation and monitoring of natural resources and their application in territorial planning and governance. *Geology in China*, *49*(4), 1048-1063.

Zhang, Y. (2022). Security issues and defences for Internet of Things.

Zhu, S., Yu, T., Xu, T., Chen, H., Dustdar, S., Gigan, S., ... & Pan, Y. (2023). Intelligent computing: the latest advances, challenges, and future. *Intelligent Computing*, *2*, 0006.

7. Appendix

7.1 Questionnaire

7.1.1 Section A - Demographic Information

Please complete the information below. All answers are kept private and will only be utilized for academic research.

I. Age

- 18 to 24 years old
- 25 to 34 years old
- 35 to 44 years old
- 45 to 54 years old
- 55 and above

II. Gender

- Male
- Female
- Prefer not to say

III. Highest Educational Qualification

- Professional Certification (e.g., CEH, CISA, CISSP)
- Bachelor's Degree
- Master's Degree
- Doctorate (Ph.D.)
- Other (please specify): _____

IV. Current Role / Job Title

- IT Manager
- Cybersecurity Analyst
- Information Security Officer

- Risk Officer
- Security Engineer
- Network Administrator
- Other (please specify): _____

V. Years of Experience in IT / Cybersecurity

- Less than 2 years
- 2 to 5 years
- 6 to 10 years
- 11 to 15 years
- More than 15 years

VI. You're Company's Primary Technology Focus (you can choose more than one):

- Artificial Intelligence (AI) / Machine Learning (ML)
- Internet of Things (IoT)
- Blockchain Technology
- 5Gnetworks
- Cloud Computing
- Quantum Computing
- Other (please specify): _____

7.1.2 Section B – Research Questions

Please use the following scale to indicate how much you agree with each statement:

1 – Strongly Disagree, 2 – Disagree, 3 – Neutral, 4 – Agree, and 5 – Strongly Agree

Questions	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)

Classification of Major Cybersecurity Risks					
Our company has a large collection of cybersecurity risks related to emerging technology.					
Our risk management strategy is improved by identifying particular threat vectors, such as phishing, DDoS, and APTs.					
More efficient use of resources for risk mitigation is facilitated by clearly defined risk categories.					
We regularly update our risk classification system to take into account new threats.					
Stakeholders understand how different cybersecurity risks are classified and what they mean.					
Technological Vulnerabilities					
Within our company, AI systems pose serious cybersecurity risks.					
Our cybersecurity posture is continuously threatened by unpatched IoT devices.					
The security of our company has been directly damaged by cloud misconfigurations.					
Our vulnerability is increased by the intricacy of integrating new					

technologies.					
To find and fix technological flaws, vulnerability assessments are carried out on a regular basis.					
Effectiveness of Cybersecurity Frameworks					
Our organization follows a recognized cybersecurity framework (such as NIST or ISO 27001.					
The cybersecurity frameworks in place are efficient in identifying and handling incidents.					
As technology advances, risk assessment procedures are periodically examined and modified.					
Our cybersecurity framework establishes criteria that employees are instructed to follow.					
Our organization is currently more cyber resilient overall because of the cybersecurity architecture in place.					
Targeted Cyberattacks					
We have been considered the victim of cyberattacks that explicitly take advantage of new					

technologies.					
With the right preparation, our cybersecurity infrastructure can resist targeted attacks.					
Tech-based dependencies are often exploited by social engineering tactics.					
Plans for incident response have been established to efficiently handle targeted cyberattacks.					
Security measures have been upgraded as a result of lessons learned from previous targeted attacks.					
Organizational, Technical, & Regulatory Challenges					
Regulatory modifications often fail to keep up with the rapid advancement of technology.					
It is still difficult to integrate cybersecurity across corporate units.					
Advanced security measures are difficult to adopt due to technical limitations (such as older systems).					
We are unable to properly address issues related to cybersecurity due to a lack of resources.					

For our firm, adhering to various regulatory standards presents substantial challenges.					
Governmental & Industrial Preparedness					
National cybersecurity regulations offer adequate direction for risk management in developing technologies.					
Our company's cyber resilience has been reinforced by industry relationships.					
Threat mitigation is accomplished quickly and efficiently by government incident response teams.					
Collaborations between the public and private sectors have improved our preparedness to deal with cyberattacks.					
Our knowledge regarding emerging cybersecurity issues is enhanced by our involvement in industry forums.					