ASSESSING THE IMPACT OF EMERGING TECHNOLOGY ON ENTERPRISE INFORMATION SECURITY

by

MANJU DEVARAJ
Msc.D, MS, BE

DISSERTATION
Presented to the Swiss School of Business and Management Geneva
In Partial Fulfillment
Of the Requirements
For the Degree

DOCTOR OF BUSINESS ADMINISTRATION

SWISS SCHOOL OF BUSINESS AND MANAGEMENT GENEVA

March, 2026

ASSESSING THE IMPACT OF EMERGING TECHNOLOGY
ON ENTERPRISE INFORMATION SECURITY

by

Manju Devaraj

Supervised by

Ivica Katavic, PhD

APPROVED BY

Anna Provodnikova, PhD

Dissertation chair

RECEIVED/APPROVED BY:

Renee Goldstein Osmic

Admissions Director

Acknowledgements

I am deeply grateful to my mentor & guide & all others who have been motivating me directly & indirectly, with special mention of Dr. Ivica, who has been very patient with me throughout. Thanks for his directions that helped me move forward.

ABSTRACT

ASSESSING THE IMPACT OF EMERGING TECHNOLOGY ON ENTERPRISE INFORMATION SECURITY

Dr. Manju Devaraj
2026

Dissertation Chair: <Chair's Name>
Co-Chair: <If applicable. Co-Chair's Name>

This research study investigated the impact of emerging technologies, which are Artificial Intelligence (AI), the Internet of Things (IoT), and Blockchain, on enterprise information security & its posture, with emphasis on cybersecurity incidents, vulnerabilities, leadership influence, and organizational resilience. Using a mixed-method design comprising systematic literature review, case study analysis, and quantitative survey data analyzed through correlation and regression techniques, along with methods like SWOT & Triangulation methodology, the findings from the research demonstrate that technology integration depth, rather than adoption alone, is a significant predictor of cybersecurity incidents and vulnerability exposure. The results further indicate that cybersecurity leadership influences security outcomes indirectly by enabling structured, governance-driven adoption practices. Among all the examined variables in the research, the strength of proactive cybersecurity frameworks emerged as the most significant predictor of organizational resilience, exceeding the impact of policies or leadership in isolation. Security policies showed a context-dependent relationship with incident outcomes and were

insufficient without a proper, proactive governance-driven framework. Finally, research concluded that effective enterprise information security with an emerging technology environment requires a planned, governance-led integration supported by proactive adaptive cybersecurity frameworks, providing empirical guidance for secure digital transformation.

Keywords:

Artificial Intelligence, Internet of Things (IoT), Blockchain, Governance, Resilience, Leadership, Emerging technology

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Enterprises are continually seeking innovative approaches to address complex business challenges and enhance operational efficiency. A planned approach is required to adopt emerging technologies (ETs) like Artificial Intelligence (AI), the Internet of Things (IoT), & blockchain. While these technologies create a greater impact on the information technology (IT) functions, helping to redefine & reshape how IT systems are developed, deployed, and managed, they also introduce new and complex information security challenges.

With novel technologies, there's a challenge in using generic or older standards & frameworks that don't accommodate or understand their dynamics. A good example of this is the transformation from physical servers to Virtual machines (VMs), from VMs to containers/pods, and so-called microservices. The standards also had to evolve as technology evolved, but it always takes time for newer standards to be published, especially in the case of the International Organization for Standardization (ISO) & National Institute of Standards and Technology (NIST), as they follow revision cycles for the updates to be released as part of the revision which might become a concern in case of a very dynamic scenarios.

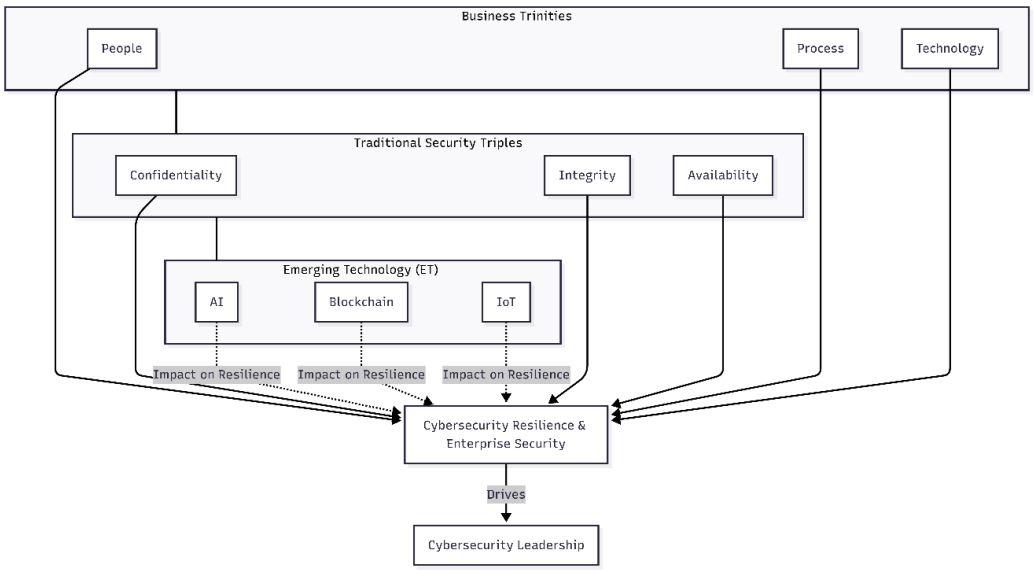


Figure 1.1

Trinities of this Research—Business, ET & Security Triples

Information security has traditionally relied on three security principles: Confidentiality, Integrity & Availability (CIA). These principles have been the fundamentals for assessing the Enterprises of any organization, but they might no longer suffice in the current context, especially with the adoption of newer technologies or technological evolution. As these technologies evolve, strategies & frameworks must evolve to be adaptable.

As we know, technology & people alone don't make it complete without processes, so it's equally important to address the human factor through appropriate upskilling & training to ensure they are aware of newer technologies & the challenges they bring. In this case, the trinity of business, so-called people, process & technology must be aligned to work towards common goals of business to maximize the benefits of technology adoption & to be competitive & successful in the market. Business resilience should ensure cyber resilience & Digital Leadership strategies to survive in the digital age.

The digital era has posed an unprecedented challenge, driven by rapid technological changes & the new risks, and the challenge of adoption without proper preparation & a plan, which raises the question of how effective Enterprise Risk Management (ERM) is in such cases. Ideally, an enterprise's security targeting cybersecurity resilience is driven by a robust cybersecurity leadership program that includes strategies & practical frameworks that not only drive the security culture but also ensure enterprises adopt security-by-design & privacy-by-design principles, along with practices like security as a default, to complement the primary security principles, which are Confidentiality, Integrity & Availability (CIA). Maybe there is a need for additional security attributes & principles during the integration & implementation of newer technologies, such as blockchain, that demand beyond the basic coverage provided by security triples.

Enterprises are constantly under pressure to embrace these technologies to stay competitive, but safeguarding their digital assets from emerging threats has been a significant challenge. Technological advancements often outpace the development of robust security measures; there is no proper strategy to address this issue.

In summary, most organizations adopt new technologies early without ensuring that their cybersecurity strategies can effectively address & manage the associated risks.

Proper planning is required before adopting or integrating any new technology. This study aims to explore the impact of the adoption of emerging technologies on enterprise

information security by identifying all the key risk factors, vulnerabilities, challenges, and gaps in the current frameworks & strategies, evaluating the role of leadership & Governance in mitigating all challenges, and proposing new or strategic solutions and proactive frameworks to enhance cybersecurity safeguards and security measures. This thesis will henceforth was built upon the research proposal and the literature review outcomes, with a keen focus on the results of the research outcomes driven through the statistical & a triangulation methodology, followed by recommendations on newer models, strategies & frameworks to address the limitations & gaps in the current context of any newer technology adoption & the impact it can have on cybersecurity & information security.

1.2 Background

The field of enterprise information security and cybersecurity has been significantly impacted in both directions, primarily due to the adoption of novel technologies such as artificial intelligence (AI), the Internet of Things (IoT), and blockchain. With the adoption of newer digital technologies, the foundational business trinity of people, process, and technology is transformed, creating both new opportunities and complex security challenges for modern enterprises.

While these newer technological innovations help unlock unprecedented efficiencies and insights, giving powerful capabilities to automate operations, enhance efficiency, strengthen analytics, and improve decision-making, they have also introduced novel attack vectors due to early adoption or unplanned integration, thereby increasing enterprise vulnerability, with the introduction of systemic vulnerabilities that traditional security models are no longer equipped to manage systems post integration.

The dual situation they create, where they support innovation on one hand while the other side risks grow in parallel, highlights critical gaps in culture, governance, operational maturity, and organizational readiness, as threat actors leverage AI-driven attacks, supply-chain infiltration, and advanced social engineering, the challenge for enterprises is no longer limited to implementing strong controls, it now requires orchestrating secure behavior, resilient processes, and adaptive systems across the entire organization to be able to keep themselves secured against such threat vectors.

So, it's inevitable that Technology enables business but cannot sustain without proper leadership

strategies & frameworks. Technology can be a catalyst for business when it's coupled with a proper acquisition plan & strategy to manage it well. Cybersecurity leadership is driven by strategies that champion security, such as a security-first culture, security-by-design, adaptability & continuous learning. Leadership must drive integrated frameworks that are adaptive & scalable, with a workforce that understands them and is empowered to drive excellence, and the right systems & people that make things work as required. Cybersecurity Leadership should adopt integrated system models that can adapt to deliver business outcomes through planning, testing & innovation.

This research is an intersection of business innovation, cyber risk, and cybersecurity leadership, examining how enterprises can navigate the complexity of such adoption, balancing opportunity and vulnerability, and leveraging leadership-driven strategies to shape culture, strengthen awareness, modernize processes, and guide the secure adoption of emerging technologies.

It was confirmed in the research paper on 'Applications of Cyber Threat Intelligence (CTI)', which found that the need for proactive threat mitigation is crucial, as the fast pace of technological adoption often outstrips the development of robust security measures (Kayode-Ajala, 2023) . Further, as Ajish (2024) states, all enterprises need to stay updated and adaptive; continuous learning and adaptation are key, as they enable organizations to withstand attacks more effectively and minimize their impact. While these shifts require adaptation, they also create complex security challenges. For instance, according to Hasan et al. (2022), blockchain technology promises decentralized solutions but faces difficulties in establishing trust within multi-party transactions, and integration with traditional architecture is always a challenge.

1.3 Research Problem

Despite the rapid adoption of emerging technologies such as AI, IoT, and Blockchain, many enterprises lack a clear understanding of how these technologies reshape information security risks and controls. This gap hinders executives' ability to make informed strategic decisions, leaving organizations vulnerable to evolving threats while limiting the secure realization of technological value. While these technologies offer benefits such as operational efficiency, data integrity, and automation, they also create new attack vectors, introducing additional vulnerabilities and complex security challenges.

While many of the Emerging technologies has been helping organizations & enterprises positively, at the same time they open newer vulnerabilities & issues creating newer risks, a loose integration without running a proper pilot or proof of concept underlines the urgency for organizations to adapt without strengthening their security measures in response to the growing & evolving threat landscape; here proactive risk assessment would help understanding those integration risks which is very crucial to mitigate them before adaption of any of such newer technologies.

Further, traditional approaches & existing risk frameworks & risk methodologies, in many cases, do not correctly address issues until they are upgraded to become dynamic.

Information security protects digital assets, which always include data and systems, from unauthorized access, corruption, and theft. With the integration & adoption of novel or emerging technologies, traditional security measures are always challenged by the evolving attack landscape & new risks.

For example, AI is prone to many attacks; prominent ones include adversarial AI attacks and data poisoning (reliability-impacting).

In the context of this study & research, the focus was on Artificial Intelligence (AI), the Internet of Things (IoT), and Blockchain to narrow the scope to specifics, while other emerging technologies, such as Quantum Computing, are also gaining prominence due to adoption. These technologies have its benefits and drawbacks from a security perspective. These innovations can always introduce new vulnerabilities and risks. Hence, there is a need to exercise due care, which calls for careful integration with robust security frameworks.

To conclude, the research problem boils down to the dual aspect to ET adoption by enterprises: the positive side focused towards the three E's: efficiency, effectiveness, and excellence; the negative side impacting business trinities negatively which are people, process & technology by creating gaps & newer issues like vulnerabilities, human-centric gaps - low security awareness, cultural resistance, skill shortages, process gaps like lack of standardization, outdated framework & governance models, and ineffective incident response; technological gaps focus on legacy system, poor integration, insufficient monitoring, and inadequate implementation of modern proactive security frameworks, while the leadership gap focussing on limited insights & foresight & strategic oversight to such an adoption.

1.4 Purpose of Research

The purpose of this study is to assess the impact of emerging technologies on enterprise information security by identifying associated security risks, evaluating organizational preparedness, and analyzing mitigation strategies. The key objectives include identifying opportunities and threats posed by emerging technologies, thoroughly analyzing evolving threats, vulnerabilities, and gaps in business trinities, creating and providing a necessary proactive framework and recommendations to address these gaps, and focusing on making these technologies positively reshape and transform the IT security landscape.

Ultimately, this research was aimed at helping enterprises with the necessary knowledge, best practices, and leadership strategies to navigate the complexities of adopting new technology without compromising their enterprise security posture, while providing insights to risks & help with proactive hybrid frameworks & leadership strategies to implement the required safeguards to manage risk and protect their valuable information assets effectively, ultimately helping business to realize the benefits due to technological adoption while minimizing the risks to business, aligning with the one of primary objectives of Governance which is " Benefit realization ".

1.5 Research questions & Hypothesis

Specific research questions were designed with a well-defined purpose to guide this mixed study on emerging technology and its impact on enterprise information security and cybersecurity. Research questions & the null hypothesis (H_0) are listed below:

RQ 1: What would be the security implications and strategic decision-making challenges that an enterprise face when adopting emerging technologies?

Hypothesis ($H_0$1): The adoption of AI, IoT, and blockchain technologies increases the complexity of enterprise security management, leading to cybersecurity breaches & incidents.

RQ 2: What are the vulnerabilities and risks associated with integrating AI, IoT, and blockchain technologies into enterprise systems, and how can these be mitigated?

Hypothesis ($H_0$2): Integrating emerging technology into enterprise systems significantly correlates with increased specific vulnerabilities, such as data privacy issues and scalability concerns.

RQ 3: How does digital leadership from the information security front influence the adoption of emerging or evolving technologies, helping to secure their implementation in enterprises?

Hypothesis (H_o3): Strong information security leadership positively influences the secure adoption and implementation of emerging technologies, reducing the likelihood of security breaches.

RQ 4: What are the deficiencies in the available framework? What are the ingredients of a proactive cybersecurity framework?

Hypothesis (H_o4): A proactive cybersecurity framework may combine risk-driven strategy, strong culture and governance, and advanced technical controls with resilience and user-centric design to withstand & recover from evolving threats.

RQ 5: What policy frameworks and strategies based on industry best practices can be developed to enhance security while deploying emerging technologies in enterprises?

Hypothesis (H_o5): Implementing comprehensive security policies & frameworks, and adhering to industry best practices, significantly reduces the security risks associated with AI, IoT, and blockchain integration.

1.6 Significance of Study

The significance of this research lies in its ability to analyze & recommend solutions & frameworks by studying the impact of newer, or so-called emerging, technologies on cybersecurity posture or cybersecurity resilience. The study takes a systematic approach to understanding the problem of new technology adoption and providing necessary recommendations to address the challenges. Starting from understanding each of those technologies, how they positively impact & negatively degrade the cyber posture, the benefits, the challenges, and further moving on to the study of theoretical models, existing theoretical frameworks & their limitations to accommodate & assess the novel technology risks, to understand the current gaps in the regulatory standards, to test the impact of independent variables like leadership, adoption level, incident levels, incident types, policies, governance & frameworks against independent variables like cyber resilience, if they directly impact or indirectly influence the cybersecurity posture and the organization's cybersecurity resilience?

In most cases, organizations & SMEs live with assumptions that a good policy, along with some governance, helps, but the results of this research help to eliminate any assumptions to

be able to significantly create a meaningful implementation, which can help organizations to minimize the impact even in the case of any technology adoption in the light of digitization & digital transformation.

It's very important to align the business trinities: the people, processes & technology; human factors play a vital role, such as low cyber maturity or resistance to change, which can always undermine even the most advanced technologies, while outdated or inconsistent processes create systemic weaknesses across operational workflows. The gaps in awareness, culture, processes, and digital leadership become more pronounced than ever. Technology itself becomes a source of fragility when legacy systems coexist with rapidly evolving digital platforms that lack standardized controls. Leadership must therefore adopt a security-first, privacy-by-design, and security-by-default & security-by-design mindset that aligns business priorities with modern risk realities, promoting a culture of accountability, continuous monitoring, continuous learning, and proactive adaptation.

Further, the importance of this research lies in examining how enterprises can integrate these competing forces without compromising security parameters, empowering innovation while mitigating emerging risks, through coherent leadership strategies built on culture, awareness, modern hybrid security frameworks, and adaptive governance. The study offers a strategic foundation for minimizing impact and closing the gaps in people, technology, & process focused on cybersecurity leadership excellence, thereby strengthening the resilience of organizations and helping enterprises to navigate the future of novel technology adoption & digital transformation.

This research was critical because it goes beyond current knowledge & research to date by focusing on the impact in detail, understanding the threats & risks, including limitations in current frameworks & practices, and providing recommendations for addressing these problems in the digital age.

1.7 Definition of Key Terms

In this section, please just define the term (one sentence) and state the source of the definition.

Artificial Intelligence (AI): A branch of computer science that is focused on creating systems capable of performing tasks like humans that require human intelligence, such as learning, reasoning, and problem-solving (Cheng, 2023).

Blockchain: It is widely defined as a special form of distributed digital ledger that records transactions across a network of computers in a secure, tamper-resistant, and usually decentralized way. It groups cryptographically signed transactions into blocks, links them chronologically, and replicates the ledger across many nodes so that no single party controls it and past records cannot be easily altered (Yaga et al., 2018).

Cyber Resilience: It is the ability & capability of organization to be resilient to be able to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or any compromises on its cyber resources (Security by Design for IoT Device Manufacturers ISO 9001 :2015 TECHNICAL REPORT TEC 31328:2023, 2023).

Cybersecurity Leadership: Leadership is focused on effective Cybersecurity implementation as a primary goal, with a definite vision to drive & implement a successful cybersecurity program throughout the organization. The provision of direction, vision, and resources to develop, implement, and manage a robust cybersecurity program to protect organizational assets (Lusthaus et al., 2018).

Emerging Technologies (ET): Emerging technology refers to new or rapidly developing innovations that are not yet fully mature but are expected to have significant social, economic, or technological impact. These technologies typically exhibit characteristics such as novelty, rapid growth, high potential impact, uncertainty, and convergence across fields (LLP, 2026; Rotolo et al., 2022). In the context of this research and study, our definition of emerging technologies limits itself to Artificial Intelligence (AI), the Internet of Things (IoT), and Blockchain.

Internet of Things (IoT): A network of physical devices connected, or things such as sensors, software, and smart devices connected to the internet, enabling them to collect, exchange, and act over the data, making a dumb device from past into a smart one with capability to collect & report. This study & research investigates the application of IoT in enterprise environments to improve operational efficiency and inform decision-making.“IOT is a framework in which all things have a representation and a presence on the Internet” (Mouha, 2021).

Robust Cybersecurity Framework: Cybersecurity framework robustness should ensure it covers the required set of guidelines, policies & standards to be able to manage the cyber risks

effectively. “A comprehensive set of guidelines, policies, standards, and practices that organizations adopt to systematically manage cyber risks, aligned with their business objectives and risk appetite” (National Institute of Standards and Technology, 2024).
Proactive cyber defence represents a shift from reactive incident response to predictive, preventive, and intelligence-driven security practices **(Hasan et al., 2025).**.

1.8 Summary

This research examined the impact of emerging technologies (Artificial Intelligence (AI), the Internet of Things (IoT), and Blockchain) on the enterprise’s information security posture. Organizations that adopt these novel technologies to drive efficiency and maintain a competitive edge face new and complex challenges, including cybersecurity threats and data privacy concerns.

The research aims to address not just the knowledge gap but also the gap in industry practices & best practices to help the industry sail through those challenges. This gap is addressed by thoroughly exploring the potential implications of adopting and integrating novel technologies in current and future enterprise settings. By focusing on the strategic leadership and security dimensions, the study provides a comprehensive understanding of how organizations can effectively integrate or safely implement newer technologies like AI, IoT, and Blockchain into their operations while mitigating associated risks, and also provides future directions on how to mitigate any evolving technology risks through some of the best strategies for the digital era.

The importance of this research lies in its potential to reinforce the need for a proper strategy to tackle risks & to educate enterprises & security workforce about the complexities of adopting newer technologies. The study would serve as a compass for decision-makers and technologists in the process of adopting emerging technologies. Additionally, it aims to enrich the field of business strategy and technology risk management, providing valuable perspectives for practitioners and academics.

CHAPTER 2

REVIEW OF LITERATURE

2.1 Introduction

The two essential aspects of this research were emerging technology and its impact on enterprise information security posture. The literature & articles reviewed were selected based on the defined criteria under the Systematic Literature Review (SLR) Methodology. This literature review highlights the impact of emerging technologies (ET) on information security, focusing mainly on early adoption of novel technologies, their risks due to lack of proper planning and governance, current gaps in frameworks, culture, and leadership, followed by solutions that can minimize the impact & risks for such adoption.

The novel technologies featured in this research, classified as Emerging, can deliver innovation, greater efficiency, automation, and valuable data insights for enterprises. However, if not properly managed and governed, it introduces additional risks to organizations, posing significant security challenges and vulnerabilities. In this literature review (LR), we have adopted a systematic approach using the PRISMA guidelines, as per Parums (2021) , this approach will ensure comprehensive coverage and minimize bias.

2.2 Evolution of Emerging Technology & its Adoption

Let's dwell on the evolution of these technologies to better understand them, looking at them from their historical & maturity context.

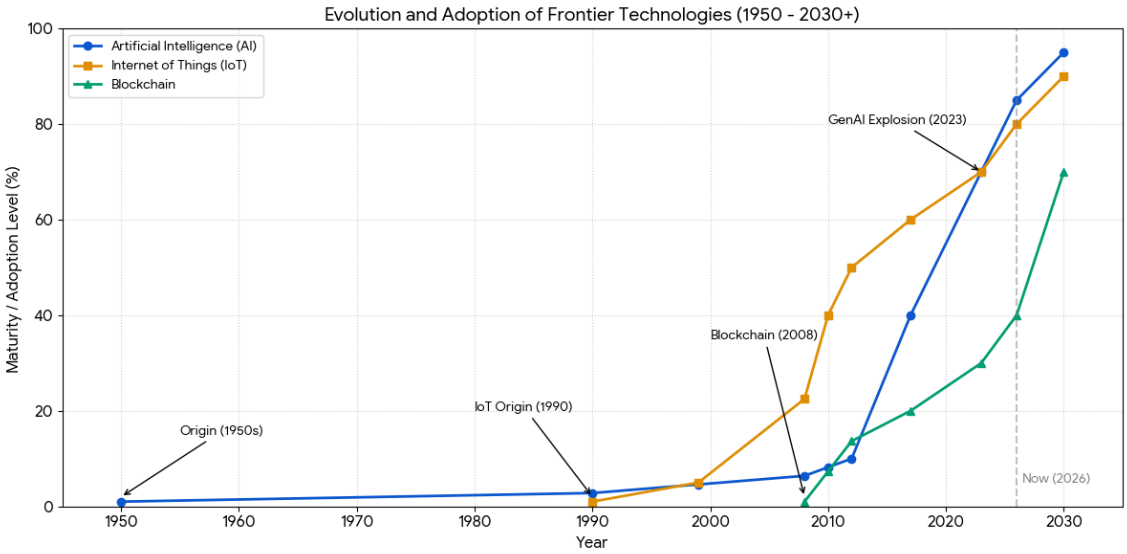


Figure 2.1

Evolution of Emerging technologies (AI, IoT, Blockchain)

As shown in the figure above, among emerging techs, the AI Journey is the longest. AI was conceptualized by McCarthy in the 1950s. AI spent years together before the year 2012 deep learning breakthrough & the year 2023 generative AI explosion. AI would stand as a good example among the emerging technologies that showed an higher & faster impact on IT post the Gen AI's explosion in 2023, as we have experienced that many of the routine tasks & roles have been replaced by AI agents now, also content writers have been challenged by generative AI, it also has positively impacted technological solutions to move to next level, such include threat hunting & threat detection technologies like IDS, Anti-malware & IPS as they have moved to real-time behavioral from traditional signature based methods, while AI has been helping in complete task automation, predictive analysis & other areas, it also has opened up challenges due to inherent vulnerability in the AI models opening up security issues & risks for enterprises adopting them few of those are AI usage for hacking systems & creating deep fakes videos to fool people.

Similarly, the Internet of Things (IoT) first interconnected Toaster appeared in 1990 & the term was coined in 1999, but mass adoption only happened in 2010 with the surge in smartphone adoption and the affordability of sensors, while the rapid adoption of such devices under Industrial 4.0 & Smart Homes raised concerns as these devices lacks computing resources to provide enough security has been a major concern for many years along with vendor specific

implementations, 21+ Billion endpoint devices were noted to be active which brings in a great opportunity for hackers & concern around the security of these. While Blockchain was introduced by Satoshi Nakamoto in 2008 under the Bitcoin Whitepaper, one decade was spent only on currency, before it evolved into Blockchain 2.0, where the Smart Contract feature was introduced, which led to its wider adoption of technology, even though the technology is known for higher security with immutable ledgers, in also inherently suffer' s due to issues & vulnerabilities like Oracle problem in case of real world asset(RWA) tokenization, also in case of Supply chain ledgers use blockchain to provide one version of truth, but that truth is only as good as data entered into it, this is also called 'Garbage in & Garbage out '.

Blockchain based systems, enhances security & integrity through decentralized approach through a method called consensus eliminates a single point of failure while one of the major problem is the scalability & performance in case of growing nodes & transaction can be hefty on storage & can cause latency issues along with high energy use in case of Proof of work, last but not the least is the integration with legacy systems & connecting heterogenous blockchains are always challenging (Alghamdi et al., 2024; Tripathi et al., 2023) , while IoT excels itself in smart homes, smart cities, industrial automation, and smart grids enables real-time monitoring, remote control, and predictive maintenance, improving efficiency and reducing operational costs his been major player in the industry as Industrial IoT, in agriculture & in healthcare (Aouedi et al., 2024).

According to Uddin et al. (2020), a significant problem with the rapid & wider adoption of emerging technologies, such as Artificial Intelligence (AI), the Internet of Things (IoT), and Blockchain, concerns the lack of development of the required information security measures. As stated in UpGuard's data breach guide, a data breach is the outcome of a planned cyber-attack. Further, it recommends that enterprises protect against data breaches by leveraging continuous attack surface discovery, AI-powered Threat Intelligence, and well-planned, smart workflows & integrations.

So we have learned that with any emerging technology, it's evident that, as they help businesses in many ways by solving business problems, they also introduce new complexities, such as vulnerabilities and risks, current silo non-innovative approach doesn't solve these problems until newer strategies & hybrid proactive frameworks are created to solve such problems but the question why these technologies gets adopted the moment there is positive

trigger on such, when the technology existed for many years, the rush to use or adopt should be delayed by the right leadership strategies which doesn't let enterprises adopt it without a proper plan.

Emerging Technology Challenges

As per Trung et al. (2021), "when new programs are emerging, there is no coherent and holistic approach to horizontal cyber security issues, for example, in the field of IoT. Existing programs have significant shortcomings and differ in terms of the scope of the products they cover, levels of assurance, substantive criteria, and actual application, hampering mutual recognition mechanisms in the European Union." (Trung et al., 2021).

Further, Omolara et al. (2022) highlighted the lack of comprehensive studies addressing the security aspects of IoT in the existing literature. There has been considerable research and examination of the state of IoT affairs, despite a substantial gap in exploring its security landscape from diverse perspectives in today's global environment. There are numerous studies and research papers shedding light on various aspects of emerging technology; however, no single paper comprehensively covers all the security aspects of these technologies in depth, as stated by Macedo et al. (2019), "All potential vulnerabilities can be categorized into seven domains. Still, the most discussed categories of vulnerabilities are technical and ethical. Few protocols or preventative actions exist for reducing vulnerability in any of the categories" (Macedo et al., 2019, p.2). Further research by Kelly et al. (2022) shows that no single risk framework currently exists for evaluating all emerging technologies; however, certain pre-existing models can be applied with differing levels of effectiveness based on the technology's adoption stage and the nature of the risk assessment being conducted, such as general or specific assessments like cybersecurity framework(CSF) (Kelly and Chan, 2022) .

Finally, enterprises adopting emerging technologies such as AI, IoT, and blockchain often overlook critical security aspects, resulting in an increased attack landscape & threats (Trung et al., 2021) and security deficiencies (Uddin et al., 2020). The main issue is the lack of strategic planning due to an inherent rush to adopt, which leads to unforeseen challenges (Lewallen, 2020) , due to a fragmented approach to research (Mogadem et al., 2021), and a lack of comprehensive frameworks leaves organizations vulnerable (Kelly et al., 2022). Systematic & controlled research is essential to address emerging technology-specific vulnerability domains and security issues (Omolara et al., 2022), enabling organizations to identify emerging threats and formulate effective

integration strategies to secure technology adoption and build resilient business architectures, leading to growth & Success.

AI, IoT, Blockchain, and other emerging technologies, such as Quantum Cryptography, are driving significant changes in enterprise security, necessitating comprehensive and critical study. The above claim is supported by Osmani (2023) in the report on AI. He firmly believes that AI will bring a seismic shift in terms of potential across all areas of the economy. Further, Manu (2024) presents the idea that disruption brings about a profound transformation that shakes the foundations of established orders, opening the way for a new era and driving a seismic shift in the existing paradigm, which challenges the status quo and propels progress forward (Manu, 2024).

The current research study confirms the need for a strong emphasis on proactive and adaptive strategies. Recent work highlights that traditional, static control sets are insufficient where technology adoption cycles are short & dynamic, and threat actors continuously innovate; instead, organizations must invest in continuous monitoring, threat intelligence, and iterative hardening as part of enhanced cybersecurity strategies so that security capabilities evolve alongside new deployments (Eswaraiah et al.; Hasan et al., 2025).

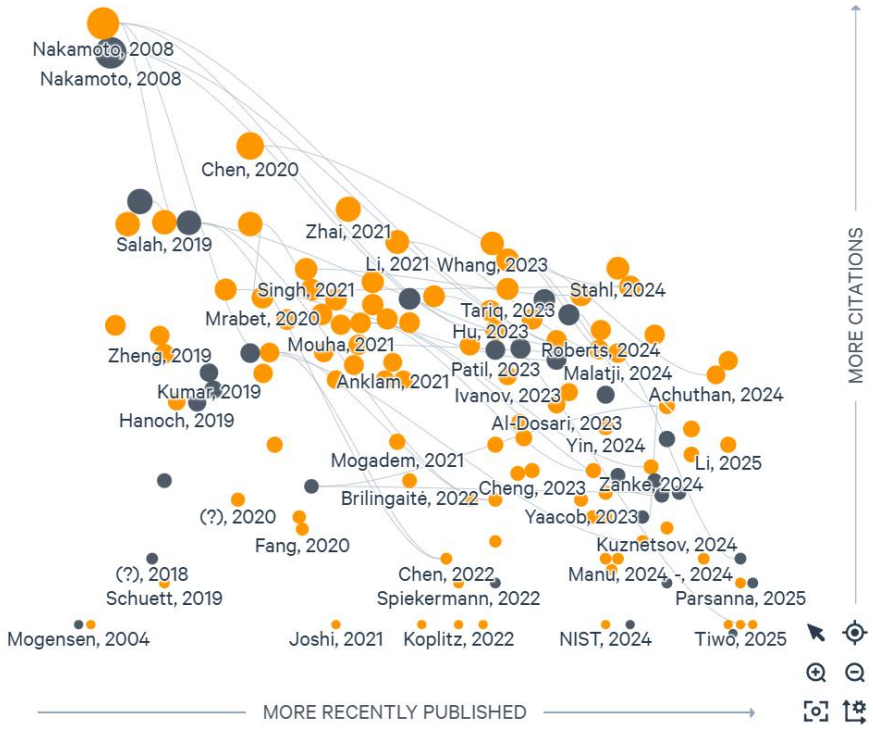


Figure 2.2

Literature Research Map

The Figure above on the Literature Map shows the scale of literature reviewed over time & its impact. Literature is considered older solely because it originates from the technology's original developer.

Blockchain can ensure data integrity via decentralization, as per Zubaydi, H.D. et al. , Blockchain Technology can be Leveraged for Ensuring Security and Privacy Aspects in Internet of Things. Blockchain–IoT integration, noting blockchain's decentralized, tamper-resistant ledger can improve security and privacy, but also presents challenges such as storage capacity/scalability, resource utilization, and transaction-rate scalability when integrating blockchain with IoT (Zubaydi, Varga, and Molnár, 2023) .

While Blockchain can add complexity/scalability and security issues, as justified by Singh, S. et al., while blockchain provides decentralized data management and integrity, it is itself subject to security attacks on consensus and smart contracts and faces scalability and performance limitations in distributed IoT networks (Singh, Sanwar Hosen, and Yoon, 2021). Blockchain could enhance integrity via decentralization but introduces complexity, scalability constraints, and its own security vulnerabilities (Mrabet et al., 2020). Further, the Global Digital Trust Insights Survey 2023 by PricewaterhouseCoopers highlights that while companies rapidly adopt AI, cloud & other technologies, many lag in implementing adequate cybersecurity controls (PricewaterhouseCoopers, 2023).

2.3 Documentation /Inclusion Criteria

The literature search strategy for this study used a structured literature review (SLR) with PRISMA to gather comprehensive and relevant information from relevant literature(focus) on the impact, intersection, and influence of emerging technologies such as Artificial Intelligence (AI), the Internet of Things (IoT), and Blockchain on enterprise information security. The search uses academic databases, including Google Scholar, JSTOR, IEEE Xplore, and ScienceDirect, to access peer-reviewed journal articles, conference proceedings, and technical reports. Search criteria included terms using Boolean logic, such as "Artificial intelligence & cybersecurity," "IoT security risks," "Blockchain & information security," and "emerging technology impact on enterprise security." These were used to find relevant studies for this research. Sources are not limited to academic databases and library resources through institutional portals; access to specific journals such as the Journal of Cybersecurity, IEEE Security & Privacy, and the Journal

of Business Economics and Finance was also used. We prioritized recent publications and foundational works to capture the latest technological developments and long-standing theoretical perspectives. The references include empirical studies, theoretical & practical frameworks, policy, and case study analysis that focused on the adoption of specific emerging technologies and their notable impact on cybersecurity and information security.

Table 2.1

Summary Table - Nature and Sources of References

Author(s)	**Nature of references**	**Sources**
Achuthan et al. (2024)	GenAI for cybersecurity: opportunities and deepfake-driven threats	Frontiers in Big Data
Ajish (2024)	Continuous Threat Exposure Management in banking	International Journal of Current Science Research and Review
Akhtar & Rawol (2024)	AI powered security mechanisms	IT Journal Research and Development
Akinsanya, Adebayo & Oshin (2024)	Cyber resilience: detection, response, recovery	Journal of Information Security and Applications
Giudici, Centurelli & Turchetta (2024)	AI risk measurement methods	Expert Systems with Applications
Godulla, Hoffmann & Seibert (2021)	Deepfakes: implications for information security	Studies in Communication and Media
Habbal, Ali & Abuzaraida (2024)	AI TRiSM: trust, risk and security management	Expert Systems with Applications
Hasan et al. (2022)	Blockchain in smart grids: security challenges	Wireless Communications and Mobile Computing
Kuznetsov et al. (2024)	Zero-Knowledge Proofs for blockchain privacy	arXiv (preprint)
Mbah & Nkechi (2024)	Balancing AI driven threats with data protection laws	Journal of Information Privacy and Security
MÄ±zrak (2023)	Integrating cyber risk into strategic management	Journal of Business, Economics and Finance
Mueller et al. (2023)	Cyber operations amid Russia Ukrainian war	CSIS Report (policy report)
NIST (2024)	Cybersecurity Framework (CSF) 2.0	Standard / Framework (NIST CSF 2.0)

NIST (2024)	AI Risk Management Framework (AI RMF & GAI profile)	Framework / Guidance (NIST)
PricewaterhouseCoopers (2023)	Digital Trust Insights: board/CEO cyber actions	PwC Report
Radanliev (2024)	AI & blockchain risks in IoT	Internet Technology Letters
Rasmussen & Hougan (2024)	Deepfakes & fraud in enterprise scenarios	Bitwiseâ€"Crypto Use Cases 2024 (industry report)
Sangwan, Badr & Srinivasan (2023)	Cybersecurity for AI systems survey	Journal of Cybersecurity and Privacy
Singh, Hosen & Yoon (2021)	Blockchain security attacks & limits in IoT	IEEE Access
Sutton & Tompson (2024)	Cybersecurity culture behavior framework	Computers & Security
Tamvada et al. (2022)	Industry 4.0 risks in emerging economy SMEs	Technological Forecasting and Social Change
Triplett (2022)	Human factors in cybersecurity leadership	Journal of Cybersecurity and Privacy

2.4 Theoretical Framework and Conceptual Frameworks

The study on theoretical framework was focused on the strengths & limitations of this framework & the applicability of those in the current context with emerging technologies, with a particular focus on the use of artificial intelligence in enterprise information security. We will map and compare key standards, guidelines, and models used to structure AI risk assessment, governance, and control in organizational settings, providing an integrated view of the current framework landscape (Habbal et al., 2024; Giudici et al., 2023).

The landscape of enterprise information security has been very dynamic, and it has evolved rapidly as organizations increasingly adopt emerging technologies such as Artificial Intelligence (AI), the Internet of Things (IoT), and Blockchain. These technologies introduce a lot of opportunities for automation, scalability, and data-driven decision-making, but they also challenge existing frameworks due to their distinct risk profiles, lifecycle complexities, and accelerated threat evolution. This necessitates a critical examination of theoretical frameworks—including RMF, CSF 2.0, FAIR, ISO/IEC standards, ERM, and cyber resilience models—to assess their suitability for emerging technology governance. Above statement is supported by

Batool in his research paper on ‘ AI governance: a systematic literature review’ , he confirms that a detailed study and understanding of the existing theoretical frameworks available are required to assess the impact of AI on security are crucial for organizations to navigate this evolving landscape effectively (Batool et al., 2025).

Emerging Technologies like blockchain & AI can be combined to improve data integrity, enable fraud detection, and enable autonomous responses to threats. According to a study by Radanliev (2024a) on ‘AI & blockchain risks’, the advent of blockchain technology provides secure data sharing and document verification at the same time. As per Farayola (2024), “technologies can be combined in the banking sector to revolutionize security, provide continuous monitoring, enable tamper-proof transactions, and deliver actionable insights” (Farayola, 2024 , p.12) , however, as per Mbah and Nkechi (2024), to accommodate data protection regulations, organizations must strike a balance between innovation and compliance, address ethical concerns, and align with privacy & security by design when conducting any data processing. We will now analyze each of the theoretical & generalized frameworks to understand their strengths and weaknesses from the perspective of the novel technology & digital era.

NIST Risk Management Framework – Generalized Framework

According to NIST standards, 'SP 800 37r2’, A Risk Management Framework (RMF) is a structured way to assess and mitigate risks for the security needs of information systems, including those utilizing AI, IoT, and blockchain technologies (Joint Task Force Transformation Initiative, 2018).

Further, “NIST Risk Management Framework (RMF) is a widely accepted and comprehensive framework for managing and mitigating risks to information. The RMF provides a structured approach to risk management, consisting of six steps: Prepare, Categorize, Select, Implement, Assess, and Maintain (National Institute of Standards and Technology (NIST), 2020) . As per Ross et al. , NIST framework has been widely adopted across various industries and sectors, including government, healthcare, finance and other sectors for managing information systems risk, despite its origins in the US federal government, the NIST RMF can be applied as a general framework for assessing risk in various contexts, including enterprise technology and information systems (Ross et al., n.d.). The framework's risk-based approach and consideration of effectiveness, efficiency, and constraints make it a valuable tool for managing risks in Enterprises and Information systems driven by traditional technologies (NIST, 2020). It needs an

update or integration with other specific frameworks in the current digital age, driven by novel technologies.

Table 2.2

Risk Management Steps, Data Source: (Gragg, 2022)

RMF Steps	**Description (NIST, 2020)**	**Application to Information Systems (IS) (Ross et al., n.d.)**
Prepare	Prepare the organization to manage security and privacy risks.	Identify the organization's mission, objectives, and IS-relevant risk tolerance.
Categorize	Categorize the system and process the information it processes, stores, and transmits based on impact analysis.	Identify the types of data and systems used in IS and assess their potential impact on the organization.
Select	Select the set of NIST SP 800-53 controls to protect the system based on risk assessment(s).	Select controls from NIST SP 800-53 that are relevant to the organization's specific IS risks and threats.
Implement	Implement the controls and document their deployment.	Implement the selected controls within the IS environment and monitor their effectiveness.
Assess	To assess if the controls are in place, operating as intended, and producing the desired results.	Conduct regular risk assessments on the IS and evaluate the effectiveness of the implemented controls.
Authorize	Senior officials make a risk-based decision to authorize the system to operate.	Obtain senior management's approval and authorization for the IS to operate.
Monitor	Continuously monitor systems and associated risks.	Regularly monitor and review the IS risk management process to ensure its effectiveness.

By applying the RMF's six steps, organizations can effectively manage and mitigate risks to their Information systems. Implementing Risk Management Frameworks (RMF) for emerging technology is challenging for Enterprises. According to MOHD NOORULFAKHRI YAACOB, SYED, and IDRIS (2023) in their research on ‘Managing Cybersecurity risks in Emerging technology’, amongst the various issues that affect Effective Risk management implementation are technical hindrances such as securing networks and securing data, organizational troubles like employee training and strategy development, and the regulatory difficulties involved, for example, in the encounter with different cybersecurity laws (YAACOB et al., 2023).

According to Aljumaiah et al. (2025) in their research on Cybersecurity risks & NIST Framework, “ NIST framework effectively covers all identified threats, suggesting it can resolve many cybersecurity issues. However, new and emerging threats may not yet be explicitly covered. “ (Aljumaiah et al., 2025).

Risk Management Framework (RMF) & its findings

Enterprises using AI, IoT, and Blockchain can benefit from the structured six-step Risk Management Framework (RMF), which provides a framework for assessing and mitigating risks. At present, implementing general RMF, however, faces technical, organizational, and regulatory challenges. Securing networks, training employees, and complying with new cybersecurity laws & risks are difficult for enterprises. Solving these problems requires board engagement, transparency, and different tailored security strategies for newer emerging technologies.

According to research by Espíndola et al. (2022), Organizational resources are relevant factors affecting the adoption of emergent technologies for risk management. Successful RMF adoption depends on both internal (organizational resilience, digital maturity, leadership support) and external (regulatory guidance, market pressure) factors (Espíndola et al., 2022) .

The integration of AI, IoT, and Blockchain enhances security on the frontline of cybersecurity through threat detection, data security, and real-time tracking. But implementation requires addressing challenges such as interoperability and standardization. To combat evolving threats, organizations must adopt robust cybersecurity frameworks, incident response strategies, and operational security measures. Security risks also increase as emerging technologies become more efficient, so the NIST RMF may no longer be completely relevant in this context but can still be used to assess & manage risks in general.

Cyber Resilience Theory

Cyber resilience is essential for all digital enterprises; according to research by Zhu (2024a), Cybersecurity has become a critical concept for organizations facing evolving cyber threats, and it is a multifaceted concern that includes game theory, control theory, and learning theory. It enables an adaptive response to threats and proactive reasoning about the adversary's behavior. It is a greater opportunity for cybersecurity that Artificial Intelligence (AI), the Internet of Things (IoT), and Blockchain technologies are being integrated, as these technologies have the potential to address the challenge of proactive threat identification and secure data sharing,

but also introduce risks and new vulnerabilities (Radanliev, 2024). According to Hausken (2020) , the interactions among numerous societal actors, such as organizations, individuals, and governments, require proper cyber resilience strategies to go beyond what has been assumed so far and to consider each in greater depth (Hausken, 2020).

As per Parker and Bach (2020a), the convergence of Blockchain, AI, and IoT can have a transformative impact on information access and security, offering high scalability and secure intellectual property protection. Responsibility for adopting newer technologies and effectively managing the associated risks must be globalized through international cooperation and cyber diplomacy. Today's traditional cybersecurity approaches are more holistic, encompassing detection, response, and recovery. Some essential components of a cyber-resilient enterprise include risk assessment, threat intelligence, incident response, and recovery planning (Akinsanya et al., 2024). Building cyber resilience capabilities relies on Enterprise Risk Management (ERM) and Business Continuity (BC). According to research by Raban and Hauptman (2018) on 'Cyber resilience, its attacks & defense capabilities,' Cyber resilience, homomorphic encryption, and blockchain focus on defensive capabilities, whereas IoT, biohacking, and HMI increase attack capabilities & attack surface.

As per Campbell (2020) in his study on 'Quantum computing & the need for resistant solutions', an attack on a blockchain-based distributed ledger and its public key infrastructure (PKI) poses a threat from quantum computing and calls for the development of quantum-resistant solutions. However, as per Akinsanya, Adebayo and Oshin (2024) , Organizations must adjust their cyber resilience strategies to evolve with the ever-changing threat landscape, thereby integrating them into organizational strategies to support sound decision-making, better resource allocation, and risk management.

As per Loonam, O'Brien, and Corcoran (2020) in the study on Strategic leadership for Cybersecurity, leadership and organizational culture are both essential for implementing cyber resilience strategies for enterprise information security. Cybersecurity strategies need strategic leaders to shape and support, and to foster a culture of cyber resilience, and to create an ecosystem-based approach to security (Loonam et al., 2020). Threats to digital cybersecurity are best protected by an organizational culture led by project managers, with cultural transformation initiated through the introduction of security practices and open discussions of risks (Dahmer, 2020). This calls for nontechnical factors, i.e, Cyber strategy, skilled personnel, and proper

communication between the security leads and the boards to make the organization cyber resilient (Vasudevan et al., 2022) .

As per Yulianto and Soewito (2023) in their research on ‘Robust security culture and resilience against ransomware’ , a robust security culture strongly supports leadership, effective communication, and employee awareness, strengthening the resilience against threats like ransomware (Yulianto and Soewito, 2023). In general, these studies demonstrate the need to incorporate cybersecurity into organizational culture as a shared responsibility, fully supported by all employees and management at all levels. Proactive measures can help enterprises bolster their cybersecurity resilience in the face of AI-driven threats, IoT vulnerabilities, and challenges with blockchain. According to the study on 'AI-driven threats' , these days AI technology is prominently being used in real-time threat detection, anomaly identification, and automatic incident response to proactively secure gaps at an organizational (Mbah and Nkechi, 2024) .

A well-developed cyber resilience should be built on a proactive Cybersecurity Framework driven by proactive strategies that focus on business continuity through risk assessment, threat intelligence, incident response, and recovery planning. AI-driven threat detection, blockchain-secured data sharing, and IoT real-time monitoring are contributing to both attack and defense capabilities. Leadership and organizational culture continually shape the implementation of the cyber resilience strategy; a good cyber resilience strategy & framework creates a security-first mindset within your organization. Cyber resilience effectively depends on companies embedding cybersecurity in their corporate culture and treating security as a group responsibility throughout. Adaptive cybersecurity strategies & framework will help enterprises improve their resilience against new cyber threats while maintaining operational excellence and regulatory compliance.

FAIR Risk Management Framework

FAIR uses quantitative methods to analyze risks. According to the Institute (2023),

“Being able to quantify cyber risk is at the core; after all, you cannot manage what you don't measure."(Institute, 2023). According to FAIR, there are two ways to manage risks: implicitly & explicitly. In explicit risk management to mitigate cyber risks, an organization aligns its cybersecurity policies with a framework such as NIST CSF, which is updated annually. FAIR uses the Value-at-Risk (VAR) model for cybersecurity & operational risk.

The FAIR data principles, which are Findable, Accessible, Interoperable, and Reusable, offer a framework for improving data stewardship and interoperability in this context. The FAIR data principles have moved from a niche concept in scientific data management to a cornerstone of modern data governance in the era of AI, IoT, and blockchain.

2.3.5 Risk and Control Self-Assessment (RCSA)

RCSA is an integral part of most operational risk management frameworks. RCSA is a quantitative model, according to the Institute of Risk Management (n.d.), “most RCSAs include a qualitative assessment of risk exposure, use an ordinal scale for probability and impact, then combine these into a simple risk matrix. These scales typically range from 1-3 (Low, Medium, and High) up to 1-5” (Institute of Risk Management, 2002).

As per the Frontiers of Computer Science, under rapid technological change, traditional frameworks are insufficient, motivating the adoption of enhanced or integrated RCSA processes for information security and digital transformation. In this way, RCSA opens the door for rapid technological change. It identifies weaknesses of current risk approaches under fast-evolving technologies and global collaboration needs, offering arguments for why classic, qualitative RCSA must be complemented by more structured, data-driven processes (Santos-Olmo et al., 2023).

2.3.6 OECD Framework for Artificial Intelligence (AI)

Let's explore the Organization for Economic Co-operation and Development (OECD) framework for AI risk management, which gives a holistic approach when compared to ISO 31000. According to the OECD, it's crucial to address & manage AI risks. This review was focused on examining the OECD framework and its potential to manage AI risks.

The framework is designed to offer a highly systematic approach to detecting, assessing, and reducing risks associated with artificial intelligence (AI) systems, but its holistic approach lacks technical depth. OECD claims on AI’s widespread development and deployment: "The widespread adoption and increasing use of Artificial Intelligence (AI) across industries have raised concerns about the risks associated with its development and deployment" (OECD, 2019, p. 12). According to the OECD, AI is transforming work environments and reshaping job roles, making preparation for labor market transitions vital considering AI developments (“Future of Work,” 2024). The framework is made up of four high-level steps: Govern, Define, Access,

Treat" (OECD, 2023, p. 15). Thus, the OECD framework still provides a comprehensive approach to managing AI risks, encompassing identification, assessment, and mitigation. The OECD Framework provides recommendations for policymakers, focusing on areas such as investing in AI research and development, fostering an inclusive AI-enabling ecosystem, and shaping an interoperable, enabling governance and policy environment for AI.

This literature review examines the strengths and weaknesses of the OECD framework and how it compares with other risk management frameworks.

The OECD has laid out some of the principles to promote the right use of AI: "AI Principles promote innovative and trustworthy AI, aligned with human rights, guiding effective AI policies across jurisdictions " (OECD, 2024, p. 2).

According to the OECD, "AI poses various risks requiring accountability from all stakeholders, and governments must monitor AI incidents to manage associated hazards" (OECD, 2024, p. 1).

The OECD framework aligns with other risk management frameworks, such as ISO 31000 and NIST AI RMF. However, there are some differences in scope, focus, and terminology. For example, the NIST AI RMF focuses more on the technical aspects of AI risk management, while the OECD framework takes a more holistic approach; the framework still covers all aspects of the AI lifecycle, from design and development to deployment.

The OECD guideline "promotes ethical commercial conduct in AI, emphasizing due diligence and risk management. The framework primarily focuses on organizational risks, without fully considering the broader societal impacts of AI systems (OECD, 2024).

According to the OECD framework, an AI system can be classified into Five Dimensions.

1. People & Planet – Human-centric approach to building AI systems, Trustworthy AI for the Benefit of Humans and the Planet.

2. Economic Context – Highlights the need for focus & context, Sector-specific policies to be developed.

3. Data & Input – Data properties and input data description to ensure privacy, inclusiveness, and fairness.

4. AI Model – Focuses on building reliable models, focused on model characteristics, Model building, and inference methods.

5. Task & Output – Focuses on the task evaluation methods & application areas.

The last step in this Frame is the process “TREAT,” which involves addressing the risks

associated with AI systems. This step is crucial in mitigating risks and ensuring the safety and security of AI systems (Madiega, 2022, p. 15). Further, the OECD framework recommends "that organizations implement risk mitigation measures and monitor their effectiveness" (OECD, 2023, p. 23). Thus, the OECD framework still provides a comprehensive approach to managing AI risks, encompassing identification, assessment, and mitigation. The OECD Framework provides recommendations for policymakers focusing on areas such as investing in AI research and development, fostering an inclusive AI-enabling ecosystem, and shaping an enabling interoperable governance and policy environment for AI.

The Strengths of this Framework is in its alignment with international standards, including ISO 31000 and ISO/IEC 23894, ensuring consistency and coherence in AI risk management. The framework is designed to be flexible and very adaptable, allowing organizations to tailor their risk management approaches to their specific needs and contexts. The framework emphasizes the importance of implementing responsible AI through stakeholder engagement and consultation, ensuring that AI systems are developed and deployed responsibly and transparently (OECD, 2024).

While it has some pros, the framework primarily focuses on due diligence and risk management, without explicitly addressing other essential aspects of AI, such as ethics and accountability. The framework offers high-level guidance but lacks clear, actionable steps for organizations to follow, potentially leading to inconsistent implementation. While the framework mentions human rights, it does not provide sufficient guidance on how to address them in AI risk management.

As shown in Table 2.3 below, the differences between the OECD AI RMF and the NIST AI Framework are that the latter is a theoretical, principles-based framework rather than a practical or regulatory one. NIST RMF & CSF are operational frameworks, so in most cases Enterprises use them to better identify, monitor & manage their security posture.

Table 2.3

OECD vs NIST AI RMF, Data sourced from (NIST, 2024; OECD, 2026).

Dimension	OECD AI Principles	NIST RMF 2.0 / CSF 2.0
Nature	A non-binding set of high-level international principles guiding responsible and trustworthy AI.	A detailed, operational cybersecurity risk management framework with prescriptive functions and categories.
Primary Aim	Promote ethical AI aligned with human-centric values (e.g., fairness, transparency, safety, accountability).	Provide structured risk processes for identifying, mitigating, monitoring, and governing cybersecurity risks.
Binding Force	Voluntary "soft-law" adopted by member nations for policy alignment.	Voluntary for industry but mandatory for U.S. federal agencies via NIST SP-800 integration.
Level of Detail	Conceptual; lacks technical or procedural implementation steps.	Actionable; offers specific controls, subcategories, and governance processes.
Scope	Societal, ethical, and policy-level AI governance across sectors.	Cybersecurity lifecycle governance across organizational systems, data, and infrastructure.

To address risks beyond traditional qualitative assessment methods, FAIR offers a quantitative approach by converting cyber risk into financial exposure. FAIR provides significant value to strategic decision-makers and supports the risk-appetite dimensions of Enterprise Risk Management (ERM) in ways that many other frameworks don't. However, its reliance on historical loss data makes its predictions less reliable for novel, unpredictable technologies such as AI and IoT, where empirical patterns and baselines are not yet fully established. Likewise, RCSA remains widely adopted for governance, but due to its subjectivity and process bias limitations, it is insufficient for highly technical or rapidly changing environments, reinforcing the need for objective, analytics-driven risk assessments (RQ1, RQ2).

Emerging challenges have prompted the need for a more flexible yet dynamic & reliable framework that emphasizes adaptability and resilience.

Cyber Resilience Theory helps organizations anticipate and withstand disruptions, especially relevant in contexts where adversarial attacks on AI or massive IoT botnets can rapidly escalate. Similarly, Dynamic Risk Assessment (DRA) frameworks provide continuous risk scoring and real-time threat detection, aligning more closely with the velocity and volume of modern attack surfaces, but the latest framework lacks the focus of the older NIST & FAIR frameworks.

In practice, the above models support RQ3 and RQ5 by enabling proactive monitoring and leadership-driven resilience strategies.

Furthermore, the proliferation of IoT ecosystems and decentralization-based blockchain infrastructures demands frameworks specifically tailored to their architectural and operational complexities. Blockchain security frameworks include aspects of blockchain technology but lack the fundamental IT components. They include consensus layer governance and smart contract assessment models, offering enhanced integrity but suffering from fragmentation and a lack of standardized enterprise-level governance integrations. Similarly, IoT security requires layered models and device-level identity controls that ISO/IEC 27001 or NIST IR 8259 only partially address. These gaps underline the need for hybrid or integrated frameworks to address all that encompasses cryptographic assurance, embedded security, lifecycle governance, and continuous monitoring (RQ2, RQ4, RQ5).

The OECD AI Principles offer a strong ethical foundation that helps enterprises understand the broader security, governance, and human-centric implications of emerging technologies, directly informing RQ1 and RQ2. Their emphasis on transparency, accountability, and fairness supports the development of effective digital leadership and proactive cybersecurity culture, addressing RQ3 and RQ4. However, because the OECD framework remains high-level and non-prescriptive, organizations must combine it with more detailed operational frameworks to meet the practical policy and risk-mitigation needs outlined in RQ5.

The critical element in the research is the emphasis on the human and cultural dimensions of cybersecurity, Cybersecurity Culture Framework, especially when combined with threat-informed models such as MITRE ATT&CK, which enables organizations to move beyond policy compliance toward behavioral resilience. Given the increase in deepfakes driven by AI, AI-driven phishing, and social engineering, culture and leadership play an indispensable role in

addressing RQ3, underscoring that technical controls alone are insufficient.

So now we can clearly demonstrate the alignment with the research questions: identifying risks of early adoption (RQ1), revealing scalability and framework gaps (RQ2, RQ4), emphasizing leadership influence and culture (RQ3), and establishing requirements for a hybrid, adaptable framework capable of measuring & governing AI, IoT, and blockchain ecosystems (RQ5). This comprehensive understanding provides a solid theoretical foundation for developing the proposed hybrid model to access technology.

2.5 Applied Conceptual & Industry Frameworks

According to Kelly and Chan (2022) , " No risk framework has yet been established specifically for assessing emerging technology, but some existing models can be used with varying degrees of success depending on the stage of the technology's adoption."(Kelly and Chan, 2022).

Further, according to the annual report by PricewaterhouseCoopers (2023b)

On 'Digital Trust Insights 2023', and its various iterations, consistently document a significant "trust deficit" between organizations' technology adoption strategies and their cybersecurity readiness (PricewaterhouseCoopers, 2023).

The above statement makes it very clear that there is one framework available for assessing novel technologies; however, flexibility is often lacking, and many frameworks are created to address a specific regulatory or technology requirement.

2.5.1 NIST AI Risk Management framework (RMF) - Applied Conceptual framework

The NIST AI Risk Management Framework (RMF), as documented under the AI RMF Playbook, provides the following functions: govern, Map, Measure, and Manage (AI RMF AI RMF PLAYBOOK PLAYBOOK, 2023).

According to Kaur et al. (2023) , Artificial intelligence (AI) is revolutionizing cybersecurity by enhancing key processes like threat detection, prevention, and response (Kaur et al., 2023).

It was noted that the use of AI within the NIST cybersecurity framework's core functions - Govern, Identify, Protect, Detect, Respond, and Recover—not only strengthens defenses but also enables proactive risk management and vulnerability assessments (Kaur et al., 2023).

However, research studies show that while "Identify," "Protect," and "Detect" receive more attention, the functions "Respond" and "Recover" remain not much explored, suggesting a gap in leveraging AI for post-incident measures (Kaur et al., 2023).

The NIST AI Framework (NIST.AI-600-1) provides essential guidelines for the development and deployment of artificial intelligence systems. It focuses on the importance of transparency, accountability, and ethical considerations in AI usage, addressing risks and encouraging best practices to enhance public trust in AI technologies(National Institute of Standards and Technology (US), 2024) .

The NIST AI Framework serves as a comprehensive resource for organizations seeking to align their AI initiatives with established standards and regulatory expectations, thereby fostering innovation while ensuring societal well-being. (National Institute of Standards and Technology (US), 2024).

According to the NIST RMF, Trustworthy AI relies on accountability. But Accountability presupposes transparency. Transparency reflects the extent to which information about an AI system and its outputs is available to individuals interacting with it, whether or not they are aware of it.

For more details on NIST AI Framework Controls, refer to Appendix C, Section 7.1 NIST AI RMF Controls.

Controls Mapped to major Security Principles:

1. Confidentiality: GOVERN 1.1, GOVERN 1.6, MEASURE 2.7
2. Integrity: GOVERN 1.4, GOVERN 2.3, MEASURE 2.7
3. Availability: GOVERN 1.5, GOVERN 6.2, MEASURE 2.6
4. Accountability: GOVERN 2.1, GOVERN 2.3, MEASURE 2.8
5. Transparency: GOVERN 1.4, GOVERN 4.3, MEASURE 2.9

AI has revolutionized threat detection and response mechanisms in cybersecurity. Mahbooba et al. (2021) highlight the importance of explainable AI (XAI) in enhancing trust management in intrusion detection systems. Using machine learning algorithms for predictive analytics and anomaly detection has improved the ability to identify and mitigate cyber threats. However, AI also introduces new risks, such as the potential for adversarial attacks during the learning phases, necessitating continuous monitoring and robust defense mechanisms (Mahbooba et al., 2021).

Key risk management frameworks are generally aligned with four top-level steps, which are Define, Assess, Treat Risks, and Govern Risk Management Processes (Common guideposts to promote interoperability in AI risk management, 2023).

2.5.2 OWASP Top 10 for Large Language Models (LLMs) & AI Assurance

The security of Large Language Models (LLMs) poses a significant concern, so organizations are facing new challenges in securing their AI systems. Traditional cybersecurity practices must be re-examined and augmented to address LLM-specific vulnerabilities, including prompt injection, insecure output handling, and model denial-of-service attacks. The literature review emphasizes the importance of proactive measures, including threat modeling, AI asset inventory, and specialized security training, to mitigate the unique risks associated with large language models (LLMs).

Table 2.4

LLM Controls

SI. No.	Control Area	Specific Controls/Considerations	Description
1	Threat Model	LLM Components and Architecture	Identify attack vectors at data entry/exit points and LLM interactions.
			Analyze security boundaries between LLM components and external systems.
		Data Classification and Protection	Classify data sensitivity and implement appropriate safeguards.
2	Data Security	Data Classification and Protection	Classify data sensitivity and implement appropriate safeguards.
		User Permissions	Manage access rights to data used by and generated by LLMs.
3	Access Control	Least Privilege	Grant only necessary access to LLM resources.
		Défense in Depth	Employ multiple security layers.
4	Training Pipeline Security	Training Data Governance	Ensure data quality and integrity.
		Pipeline Security	Protect training infrastructure.
		Model and Algorithm Security	Secure model files and training algorithms.
5	Input/Output Security	Input Validation	Sanitize user prompts to prevent attacks.
		Output Filtering/Sanitization	Filter LLM outputs to remove harmful content.
		Output Approval	Establish processes for approving LLM-generated content.
6	Monitoring and Response	Workflow Mapping	Understand data flow and system processes.
		Logging and Auditing	Implement comprehensive logging.

		Audit Record Security	Secure audit logs from tampering.
7	Testing	Application Testing	Integrate security testing into the LLM pipeline.
		Source Code Review	Review custom code interacting with LLMs.
		Vulnerability Assessments	Identify weaknesses in LLM implementations.
		Red Teaming	Simulate attacks to test security.
8	Vulnerabilities	LLM/Supply Chain Vulnerabilities	Check for known vulnerabilities in LLMs and their components.
9	Threats	Threats to LLM Solutions	Address prompt injection, data leaks, etc.
		Threats to LLM Models	Protect against model poisoning, theft, etc.
10	Supply Chain	Third-Party Audits/Reviews	Audit the security of LLM providers.
11	Infrastructure	Resilience Testing	Verify infrastructure's ability to withstand failures.
		SLAs	Evaluate vendor SLAs for uptime, etc.
12	Incident Response	Playbook Updates	Update incident response for LLM-specific attacks.
		Tabletop Exercises	Simulate LLM security incidents.
13	Performance	Performance Benchmarking	Measure the effectiveness of LLM security measures.

According to MITRE (2023) , General Distrust of AI: 82% of Americans believe AI should be regulated. Only 48% feel that AI is safe and secure(“AI Trust Gap | MITRE,” 2023).

Table 2.5 below lists the AI Controls that can provide Assurance for AI, starting from Assurance process management, flowing through system categorization to assurance life cycle implementation, covering documentation, configuration & change management aspects.

Table 2.5

AI System Assurance

Assurance Plan Aspect	**Control**	**Description**
Assurance Process Management	PM1	An instantiation of the Al assurance process tailored for the Al-enabled system. A list of the activities for completion of the assurance process and the assurance plan.
Assurance Process Management	PM2	Specification of the resources and timelines for each assurance activity, including review and approval of each activity.
Assurance Process Management	PM3	Parties who are responsible for carrying out the assurance activities and approving their outcomes.
Assurance Process Management	PM4	Description of the Al governance policies of the organization and their implications for how the Al assurance process should be applied to the mission space the Al-enabled system will operate in.
System Characterization	SC1	A description of the mission problem, the proposed Al-enabled system, and the expected use cases, scope of use, and impacts or effects of use.
System Characterization	SC2	Definition of the system needs and requirements subject to assurance through the Al assurance process, along with rationale. Requirements must be testable.
System Characterization	SC3	An assurance risk assessment that comprehensively identifies and estimates hazards and risks. Components of risks, such as their harm and their likelihood of occurrence, should be testable.
Life Cycle Assurance Implementation	LA1	Documentation and communication protocols for recording, maintaining, and sharing assurance information.
Life Cycle Assurance Implementation	LA2	A configuration management protocol that documents how the correct versions of system components and configuration parameters are managed to achieve the level of assurance that has been deemed acceptable.
Life Cycle Assurance Implementation	LA3	A change management protocol that specifies the activities necessary to change the system and determine any assurance-related consequences associated with a change in the system. Conversely, it also specifies what types of changes to the system or in its operating environment may necessitate the reapplication of the assurance process.

Life Cycle Assurance Implementation	LA4	An issue management protocol for tracking and addressing any issues that may impact assurance. This protocol specifies what needs to be tracked regarding issues, the resources required, responsible parties, methods to receive issue/incident reports, and required timelines for issue review, resolution, and validation.
Life Cycle Assurance Implementation	LA5	A system monitoring protocol that documents how and by whom the Al-enabled system should be monitored to maintain assurance. It may include continuous monitoring, automated data recording, audits, tools for performance monitoring, and monitoring of incident reports and issues. Note that monitoring should address Al assurance issues as well as any related system-level assurance issues.
Life Cycle Assurance Implementation	LA6	A verification and validation protocol of the system, used during the assurance process. This protocol documents the tests for verifying satisfaction of assurance requirements as well as the impact and likelihood of risks. Validation determines the achieved assurance level and satisfaction of assurance needs.

2.5.3 ISO/IEC 23053:2021

This is a standard that provides a framework for AI Systems that use Machine Learning. This standard is intended for use across all types and sizes of organizations, including public and private entities, governmental bodies, and nonprofit organizations that are either implementing or using AI systems.

ISO/IEC 23053:2021 emphasizes the importance of robust data management and model governance, which are essential for ensuring the reliability and effectiveness of AI-integrated information systems (IS). As stated in the standard, “AI systems using machine learning rely on data and models to achieve their intended purpose” (ISO/IEC 23053:2021, p. 5). This highlights the need for organizations to establish strong **Data governance frameworks** and implement rigorous model validation processes.

Cybersecurity risks are always being amplified by AI integration. AI-powered, automated cyberattacks can be more sophisticated and harder to detect, necessitating that organizations strengthen their cybersecurity defenses. ISO/IEC 23053:2021 emphasizes the importance of security measures to safeguard AI systems against unauthorized access, manipulation, and misuse.

Table 2.6

Controls in ISO/IEC 23053:2021

Key Controls in ISO/IEC 23053:2021		
Control Area	**Key Control Objectives**	**Specific Control Examples**
Data Management	Ensure data quality, integrity, and availability.	- Data acquisition and preparation procedures. - Data validation and verification mechanisms. - Data lineage tracking. - Data access controls and security measures. - Regular data quality audits.
Model Development & Validation	Establish robust processes for developing, training, and validating machine learning models.	- Model selection criteria and justification. - Curation and documentation of training data sets. - Model performance evaluation metrics. - Independent validation procedures. - Version control of models.
Model Governance	Provide oversight and accountability for AI systems.	- Defined roles and responsibilities. - Change management processes for models. - Documentation of model design and rationale. - Incident response procedures. - Periodic review of model performance and impact.
Explainability & Transparency	Increase understanding of AI system outputs and decision-making processes.	- Explanatory model documentation. - Methods for interpreting model outputs. - Provision of model confidence scores. - Justification for model-driven decisions. - User-accessible explanations regarding system behavior.
Fairness & Bias Mitigation	Address potential biases in data and models to ensure equitable outcomes.	- Bias detection and mitigation techniques. - Demographic subgroup analysis. - Fairness impact assessments. - Monitoring for disparate impact. - Regular testing of data and results for biases.
Security & Privacy		- Access controls and authentication.

	Protect AI systems and sensitive data from unauthorized access and misuse.	- Data encryption and anonymization. - Vulnerability assessments and penetration testing. - Incident response plans. - Compliance with privacy regulations (e.g., GDPR).
Risk Management	Identify, assess, and mitigate risks associated with AI systems.	- Risk assessments for deploying AI systems. - Development of risk mitigation strategies. - Continuous risk monitoring. - Documentation of residual risks. - Formalized change management process.
Ethical Considerations	Incorporate ethical principles into the design and deployment of AI systems.	- Ethical impact assessments. - Establishment of ethical review boards. - Consideration of societal implications. - User feedback mechanisms. - Alignment with ethical guidelines.
Verification and Validation	Processes employed to prove the system compliance and fitness of purpose	- Independent auditing procedures. - Regular system review, to determine compliance with intended purpose. - Validation of the system throughout the development and operational phases.

2.5.4 NIST Cybersecurity Framework 2.0 - An Operational Framework

The NIST Cybersecurity Framework (CSF) 2.0 has been widely adopted as a comprehensive framework for managing and mitigating cybersecurity-related risks (National Institute of Standards and Technology, 2024). Its flexibility and adaptability have made it a popular choice for organizations across various sectors, including those leveraging Internet of Things (IoT) technologies (Khan et al., 2022). A study by Khan et al. (2022) demonstrated the effectiveness of CSF 2.0 in securing IoT devices and networks, highlighting its structured approach to managing cybersecurity risk. Further, CSF 2.0 is focused not just on cybersecurity but also on its counterparts, such as ERM & Workforce Management, which is one of this framework's biggest strengths.

Moreover, CSF 2.0 has been shown to be effective in securing other emerging technologies, such as cloud computing and artificial intelligence (Sharma et al., 2020). A study by Sharma et al. (2020) found that CSF 2.0 provided a robust framework for managing cybersecurity

risk in cloud-based environments, while another study by Ahn et al. (2021) demonstrated its effectiveness in securing AI systems.

The CSF 2.0's focus on risk management and continuous improvement has also made it an attractive choice for organizations seeking to improve their overall cybersecurity posture (National Institute of Standards and Technology, 2024). A study by Lee et al. (2022) found that organizations that implemented CSF 2.0 experienced significant improvements in their cybersecurity risk management practices, while another study by Kim et al. (2021) found that the framework helped organizations identify and mitigate potential cybersecurity risks more effectively.

Traditional frameworks such as the NIST Risk Management Framework (RMF) and the NIST Cybersecurity Framework (CSF 2.0) continue to provide the foundational mechanisms for supporting enterprise IT governance, IT risk assessment, and IT control selection. RMF's structured lifecycle approach and SP 800-53 control catalog offer robust baseline security for enterprises, while CSF 2.0's Govern function strengthens strategic alignment and accountability, but misses the latest technology coverage under the framework. However, both frameworks were designed in eras preceding AI-driven decision systems, hyper-connected IoT environments, and decentralized blockchain architectures. As a result, their linear assessment cycles and static control models struggle to address fast-moving risks such as adversarial machine learning, IoT firmware exploitation, and smart contract vulnerabilities (RQ2, RQ4). These limitations highlighted the need for a more adaptive, continuous, and dynamic threat-informed cybersecurity mechanism.

Table 2.7 SWOT analysis of Theoretical Frameworks indicated that each of the frameworks comes with its own limitations, including technical, governance, scalability & flexibility, and the fixed cycle of updates on the framework outpaces changes in technology & the rapid evolution of the threat landscape.

Table 2.7

SWOT Analysis on Theoretical Frameworks

Framework	Strengths	Weaknesses	Opportunities	Threats
NIST RMF (NIST, 2020; Ross et al., 2020)	Structured 6-step lifecycle; strong governance; backed by SP 800-53 controls.	Documentation-heavy ; not optimized for AI/ML lifecycle; IoT scalability gaps (Yaacob et al., 2023).	Alignment with AI RMF, Zero Trust, SBOM/SSDF (NIST, 2024).	Rapid ET threats outpace static cycles; geopolitical escalation (Mueller et al., 2023).
NIST CSF 2.0 (NIST, 2024)	Widely adopted; strong Governance function; flexible across sectors.	High-level; requires sub-frameworks for IoT/AI (Kim et al., 2021).	Integration with AI RMF & IoT IR-8259.	AI-enabled attacks increase detection gaps; supply-chain fragility (PwC, 2023).
NIST AI RMF (NIST, 2024; Habbal et al., 2024)	Addresses trust, bias, robustness, adversarial threats in AI lifecycle.	Immature tooling; broad and non-prescriptive (Batool et al., 2025).	Forms enterprise AI Safety governance backbone.	Shadow AI undermines governance; rapid LLM misuse (Vulpe et al., 2024).
FAIR (FAIR Institute, 2023)	Quantifies risk financially; supports executive decisions.	Needs historical data; poor fit for unpredictable ET risks.	Monte-Carlo modelling for AI/IoT scenarios.	ET unpredictability lowers quantitative accuracy.
RCSA (IRM, 2002)	Simple; widely used; supports accountability.	Subjective; lacks technical depth; human bias.	Can complement RMF or FAIR.	Human-factor bias hides risks.

A Venn–SWOT, an integrative conceptual model, is used to visualize structural overlap among the stated theories & frameworks while simultaneously assessing their collective strategic implications using SWOT dimensions.

The Venn–SWOT hybrid figure below illustrates that no single framework can address the multidimensional risk profile introduced by emerging technologies; rather, we should focus on achieving resilience through purposeful integration. Governance-centric frameworks (NIST RMF

and NIST CSF 2.0) provide a robust control baseline and strategic accountability but face limitations when confronted with rapidly evolving AI- - and IoT-specific threats.

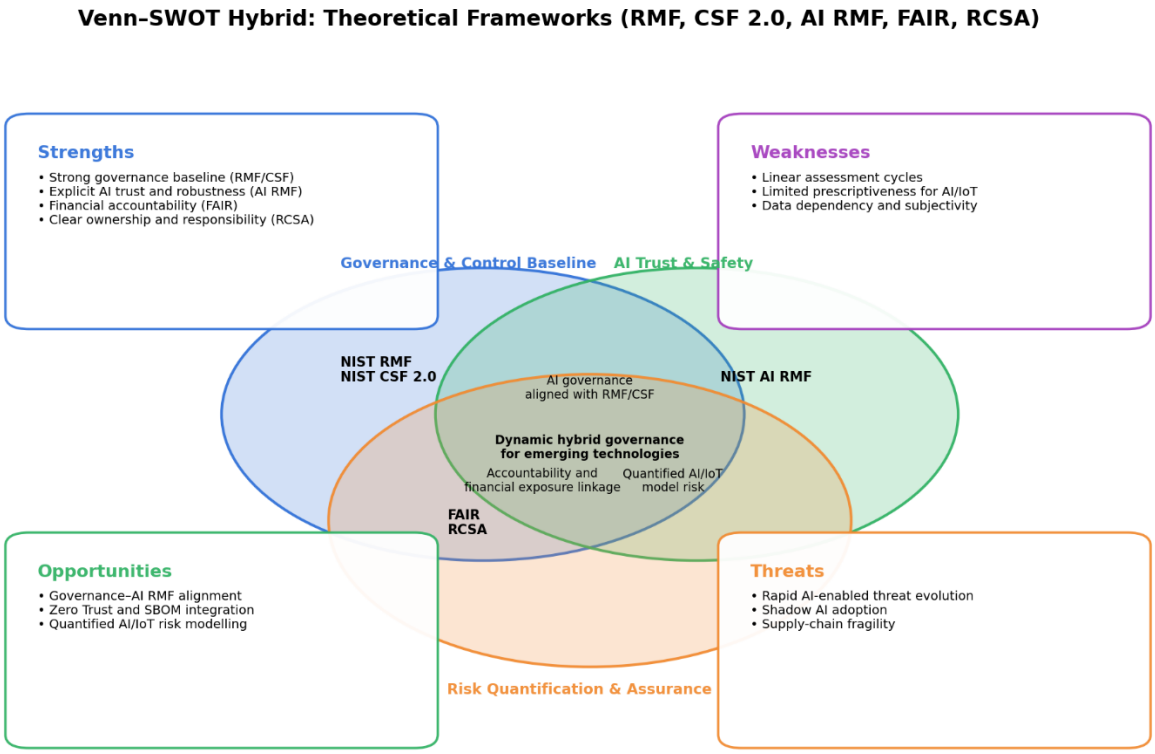


Figure 2.3

Venn-SWOT Hybrid illustration

Collectively, the figure supports the theoretical argument that an adaptive, multi-framework governance architecture—rather than framework substitution—is essential for managing enterprise risk in AI- - and IoT-driven environments.

Table 2.8

Drawbacks of the Theoretical Framework

	Framework	Drawbacks with Reference to Emerging Tech
1	NIST RMF (NIST, 2020; Ross et al., 2020)	Limited AI-specific controls; weak for IoT heterogeneity; no blockchain consensus coverage (Radanliev, 2024).
2	NIST CSF 2.0 (NIST, 2024)	Does not address ethical AI, LLM misuse, blockchain privacy (Mahbooba et al., 2021).
3	NIST AI RMF (NIST, 2024; Habbal et al., 2024)	Limited IoT-AI convergence and blockchain-AI integration guidance.

4	FAIR (FAIR Institute, 2023)	Fails to model AI bias, IoT unpredictability, or smart-contract risk (Hasan et al., 2022).
5	RCSA (IRM, 2002)	Weak for AI/ML, IoT, blockchain technical vulnerabilities.
6	Dynamic Risk Assessment (Melaku, 2023)	No structured governance layer vs RMF/CSF.
7	Cyber Resilience Theory (Zhu, 2024; Hausken, 2020)	No explicit ML-poisoning, IoT governance, or blockchain node controls.
8	Blockchain Frameworks (Komalavalli et al., 2020; Zubaydi et al., 2023)	Weak RMF/CSF integration; scalability, privacy, interoperability gaps.
9	Enterprise Risk Management (ERM) (COSO, 2017; Assibi, 2023)	Lacks technical AI/IoT/blockchain granularity without cyber-threat overlays.
10	ISMS / ISO/IEC & COBIT (ISO/IEC 27001:2022; COBIT 2019)	Lags adversarial ML controls; gaps in IoT identity and blockchain governance.
11	Cybersecurity Culture + MITRE ATT&CK (Alshaikh, 2020; Sutton & Tompson, 2024; MITRE, 2023)	Culture cannot compensate for weak controls; ATT&CK coverage ≠ prevention.

Overall, the table above's comparative analysis reveals that no single framework is adequate to address the multifaceted risks associated with emerging technologies. Traditional frameworks provide governance and structure but lack adaptability for newer implementations; quantitative models offer financial clarity but struggle with uncertainty; resilience models provide adaptability but lack prescriptive controls; and technology-specific frameworks remain fragmented to that technology only. This supports the study's proposition that a dynamic hybrid framework—combining governance (CSF/RMF), quantitative assessment (FAIR), lifecycle-specific controls (ISO/IEC, NIST AI RMF), threat-informed practices (MITRE), and resilience models—is essential for modern enterprises.

2.5.5 IoT Compliance Framework – IoTSF, ETSI & CSA IoT Controls

The IoTSF operates as a vendor-neutral and collaborative initiative, bringing together a diverse range of stakeholders from across the IoT ecosystem, including hardware and software

vendors, network providers, system integrators, distributors, retailers, insurers, local authorities, academic institutions, government agencies, security professionals, researchers, and risk managers (Foundation, 2021).

The IoTSF Compliance Framework presents several notable strengths that contribute to its effectiveness in addressing IoT security challenges. Its comprehensive coverage of various aspects of IoT security, including process, technology, communication, and physical security, as well as organizational and managerial domains, ensures a holistic approach to risk mitigation.

One drawback of IoTSF is the limited availability of publicly documented case studies that demonstrate its real-world effectiveness and impact.

Table 2.9

IoT Assurance classes

Assurance Class	**Confidentiality**	**Integrity**	**Availability**
Class 0	Little impact	Little impact	Little impact
Class 1	Limited impact	Limited impact	Limited impact
Class 2	Significant impact	Significant impact	Resist attacks on availability
Class 3	Protect sensitive data	Protect sensitive data	Protect sensitive data
Class 4	Critical infrastructure/personal injury	Critical infrastructure/personal injury	Critical infrastructure/personal injury

The table above on IoT Assurance classes helps to understand the impact of IoT systems through their classification. A Class 4 system has a higher impact with respect to CIA; hence it is classified as critical. This helps understand the IoT system and the protection measures required for it.

According to ETSI TS 103 645, developers must implement robust security measures. It highlights the importance of managing vulnerabilities actively and outlines a framework for Coordinated Vulnerability Disclosure (CVD), which facilitates communication between companies and security researchers (“CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements,” 2024) .

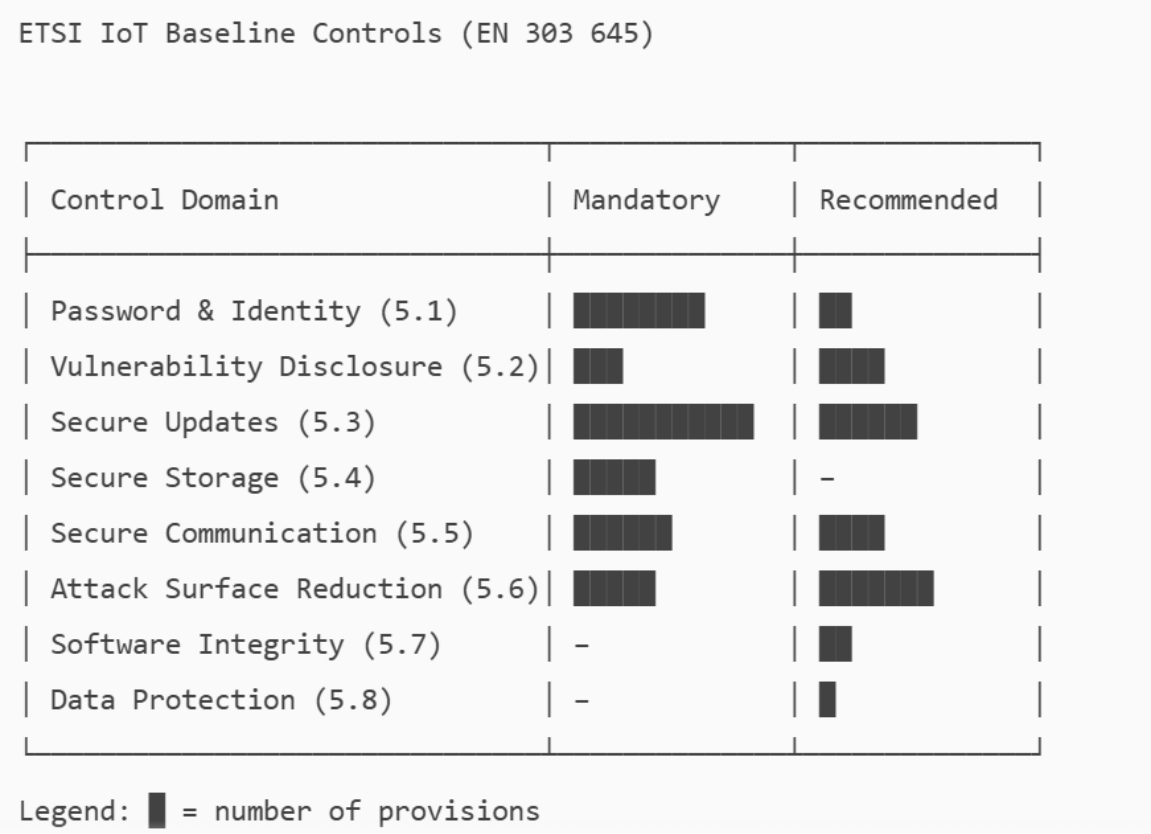


Figure 2.4

IoT Baselines Controls

ETSI EN 303 645 provides a baseline set of mandatory and recommended cybersecurity controls for consumer IoT devices, addressing identity management, secure updates, vulnerability disclosure, data protection, and attack-surface reduction to enhance accountability and lifecycle security.

For more Details on ETSI Critical Control for IoT, refer to the table in Appendix C -ETSI IoT Framework Controls. Lists controls by category: mandatory recommendations & a feature-only option.

2.5.6 CSA IoT Control Matrix for IoT Security Assessment.

CSA helps with IoT Assessment by providing the Control Matrix for IoT. A Total of around 198 controls were listed as part of the CSA IoT Assessment framework, with a major focus on IAM and the security of applications and networks.

Table 2.10

CSA IoT Controls

Control Domain	Total Sub-Controls
Asset Management	4
Configuration Management	6
Cloud Services	12
Secure Data	4
Governance	10
Identity and Access Management	22
Incident Management	14
IoT Device Security	12
Legal	9
Monitoring and Logging	11
Operational Availability	9
Physical Security	1
Policy	4
Risk Management	3
Secure Applications	16
Secure System Development Lifecycle	11
Secure Networks	14
Secure Wireless	22
Training	2
Vulnerability Management	5
Security Testing	7

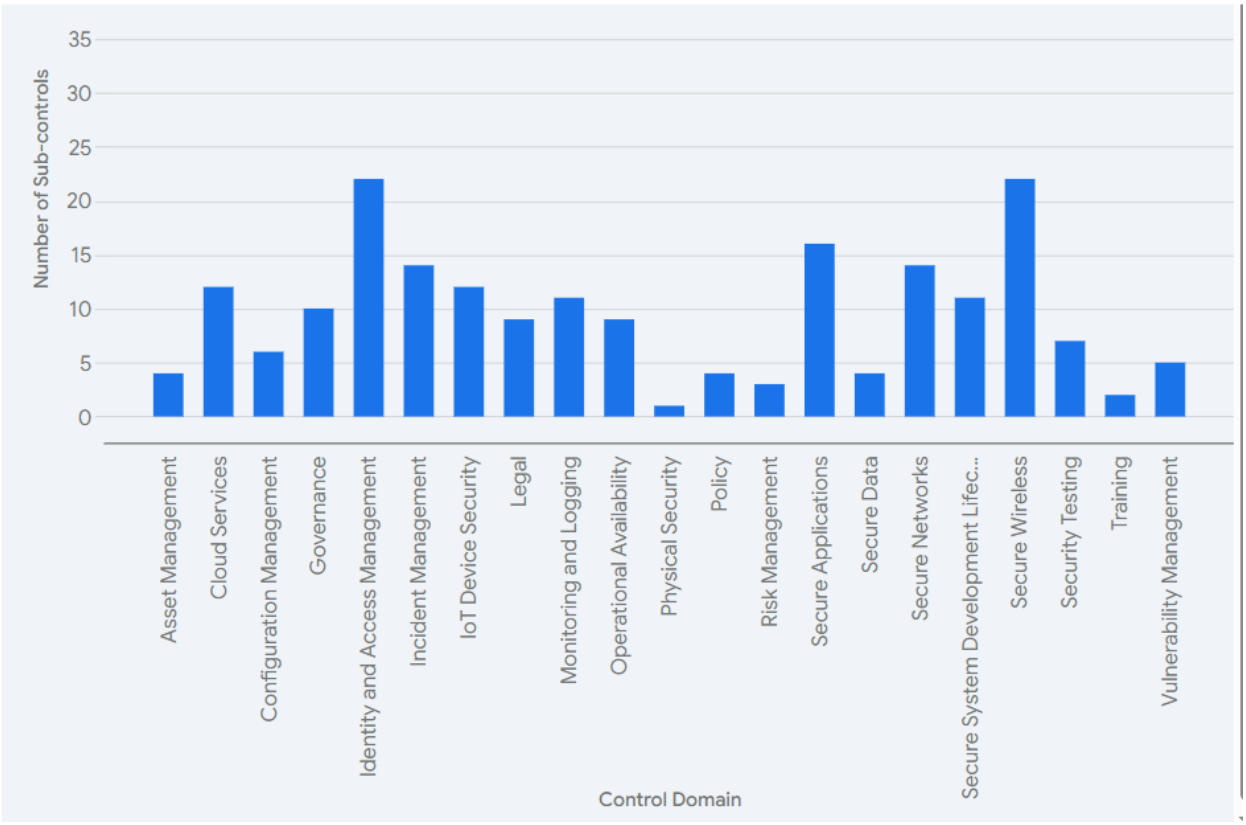


Figure 2.5

CSA IOT Control Matrix -Control Domains & Sub-controls

The proliferation of IoT devices has expanded the attack surface, making embedding security protocols from the design phase imperative. Hussain et al. (2020) discuss the challenges of securing M2M (Machine-to-Machine) communication and the need for stringent security measures. The rapid deployment of IoT devices often outpaces the development of comprehensive security frameworks, leaving systems vulnerable to breaches and incidents. The IEEE Std 2413-2019 provides an architectural framework for IoT, emphasizing the importance of interoperability and security ("IEEE standard for an architectural framework for the internet of things (IoT)," 2020).

Cybersecurity Leadership

The deployment of emerging technologies raises significant ethical and privacy concerns. Deepfakes, for instance, pose risks to data integrity and trust. Godulla et al. (2021) discuss the impact of deepfakes on information security and the need for robust verification mechanisms.

The ethical implications of AI, such as bias and transparency, must be addressed to ensure that these technologies are used responsibly and ethically (Godulla et al., 2021).

- **Proactive Risk Management and Governance**

Proactive risk management involves identifying, assessing, and prioritizing security risks and implementing appropriate controls. Mızrak (2023) highlights the importance of integrating cybersecurity risk management into strategic management. Governance frameworks like COBIT provide guidelines for evaluating, directing, and monitoring IT management activities. Continuous improvement and adaptive strategies are essential for addressing the dynamic and evolving threat landscape (Mızrak, 2023).

2.6 Insights into Emerging technology, Information Security and its Leadership

Faster integration of emerging technologies such as Artificial Intelligence (AI), the Internet of Things (IoT), and Blockchain has significantly transformed the cybersecurity landscape. This literature survey explores the multidimensional effects of these technologies on information security, focusing on compliance, risk management, and the development of robust security frameworks to address the ever-changing risk landscape.

In today's digitally interconnected world, there are always unprecedented levels of threats. This gets even worse with the use of new technology or integration. The impact of such is always dependent on its use & the maturity of the technology being used.

According to ODoherty (2023), within the dynamic realm of digital advancements, the rise of new technologies offers considerable opportunities along with significant challenges, especially in the field of cybersecurity (ODoherty, 2023). As confirmed by Saeed et al. (2023) in his paper on 'Digital Transformation and Cybersecurity Challenges', at the enterprise level, project under digital transformation shows there is a widespread adoption of cloud, big data, and distributed ledgers increases both efficiency and exposure, reinforcing the need for staged cybersecurity readiness models and governance mechanisms.

According to Habbal, Ali, and Abuzaraida (2024), existing frameworks may lack the mechanisms to instill and uphold trust in AI systems, adequately assess the associated risks of AI implementations, and effectively manage security within the swiftly evolving AI landscape.

As we learned, the development of AI was so fast that the world was not ready to absorb the impact of its use & release at the early stage, so they had to delay certain projects until there were some draft regulations & guidelines made available around it.

In the Article "Cybersecurity Trends: Emerging Threats and Technologies in the Cybersecurity Landscape" by IIT Kanpur, the following emerging technologies were highlighted as having an impact in the future: IoT & 5G, Quantum Computing, AI, and Blockchain. While AI is used to build the next generation of software & tools for threat detection, it is also used to develop malware & attacks to bypass certain protocols & systems(kanpur, 2023).

AI-empowered Virtual and Augmented Reality (VAR) is now being used as software for leisure and relaxation through its influence on the gaming community, as well as becoming a pervasive force in the realm of simulated training for various critical tasks. The risky part of this technology comes with the ability of this software to capture delicate user information concerning their activities and habits opens it up to the possibility of being abused to negatively impact consumers (Collum and Kettani, 2022).

An AI use case in patient health was demonstrated in the paper, an exemplary pipeline for an AI-enabled pHealth model, which was an AI-based predictive model. Many health care applications were based on diagnostic predictive models. According to the research, the models to assess the potential risk of food and chemicals, including the gut microbiome, are increasingly emerging, but some of them may still need certain adaptations to be applicable in standardized protocols (Anklam et al., 2022).

Digital trust insight report says, “More than two-thirds (69%) say they’ll use Generative AI (GenAl) for cyber defense in the next 12 months” (PWC, 2023, p.11).

According to the research report by Torkington (2024) published under the World Economic forum (WEC), “Emerging technologies create significant cybersecurity risks, exemplified by the projected 75 billion connected devices by 2025, each a potential vulnerability. AI, while offering defensive capabilities, also introduces new attack vectors like data poisoning. Quantum computing threatens existing encryption, demanding urgent development of quantum-resistant solutions. A critical shortage of cybersecurity professionals further exacerbates these challenges.

The shift from "security by design" to "resilience by design" is crucial for mitigating these risks" (Torkington, 2024).

2.5.1 Information Security

Everything is constantly being updated to transform itself to the next level, so are the information security model and principles, traditionally three security principles were worshipped throughout the enterprises to ensure organization assets are protected always now things have changed with a lot of dynamism, one size doesn't fit all anymore, there is need for much robust but yet a very flexible framework to embark over the journey of the usage & integration of Emerging technology into current Information technology scenarios.

Information Security Triples

Expanding the Focus on Confidentiality- Integrity-Availability (CIA) is crucial in the world of the ever-changing technology landscape.

Confidentiality: Moving beyond data protection to include privacy considerations, user control over personal information, and compliance with data privacy regulations.

Integrity: Encompassing data authenticity, ensuring data is consistent and accurate across its lifecycle, and mitigating the risk of manipulation or corruption.

Availability: Extending beyond ensuring access to systems and data to include resilience against cyberattacks, disaster recovery plans, and proactive maintenance to minimize downtime.

The traditional CIA triad (Confidentiality, Integrity, and Availability), also known as the security principles, has long been the cornerstone of information security. However, the evolving threat landscape and increasingly complex technological environment, along with the adoption of emerging technologies, necessitate a shift towards a more comprehensive definition of the CIA security principles as we continue to use the CIA. As per Samonas and Coss (2014) claim on CIA "Even in the 2020s, that is 50 years after its conception, the CIA triad will still be uniquely relevant & applicable for security

practitioners and will continue to serve as a point of reference in security management." (Samonas and Coss, 2014).

As years pass and evolving technologies emerge, the relevance factor and importance of the CIA have also changed. Björn and Niklas (2019) argue that the CIA definition lacks the flexibility to address diverse information, systems, and organizational needs. Moreover, they contend that the current definition does not adequately encompass the human impact on security, provide a comprehensive analysis of breaches and their timing, or offer sufficient justification for the necessity of security (Björn and Niklas, 2019).

This shift involves expanding the Focus and integrating newer Security principles to be able to holistically address the new technology & the evolving threat landscape due to adoption of emerging technologies like IOT, AI & Blockchain.

Further, as per Team Copado (2022), it is not good to treat other models like Distributed Immutable & Ephemeral (DIE) to be adversaries, according to him "Approaching DIE model security and CIA triad security as adversaries is a mistake that can leave holes in an Information Security program" (Team Copado, 2022).

Information Security Principles - Impact & Risk Matrix							
		X - Security Triples			Info Assurance		
		C	**I**	**A**	**NR**	**Auth**	**Impact Scores**
		D	**I**	**E**	**_**	**_**	
Y - Risk Level	Secure	0	0	0	0	0	0%
	Low	1	0	0	0	0	25
	Medium	1	1	0	0	0	50
	High	1	1	1	0	0	75
	Very High	1	1	1	1	1	100%

Figure 2.6

Proposed Information Security Principles for all Business Models & types.

State – 1 –Indicates that Principle is compromised

State – 0 – Indicates that Principle is not compromised

Table 2.11

Traditional Security Triples Vs Modern Security Triples Vs Information Assurance Principles.

	Traditional Security (CIA)	**Modern Security (DIE)**
Security Triples	Confidentiality Integrity Availability	Distributed Immutable Ephemeral
Information Assurance	Non-repudiation (NR) Authentication	

As per Table 2.11 above, the DIE model is a Security Framework for designing resilient infrastructure in case of a Blockchain; it's often contrasted to CIA in case of a Centralized infrastructure model. It improves **Availability** (via Distribution), **Integrity** (via Immutability), and reduces attack windows (via Ephemerality), but it does not directly provide Authentication or Non-repudiation.

2.5.2 Artificial Intelligence (AI)

The design of a typical AI system should include the following elements listed below.

1) **Data** is the life & the blood of an AI system. The quality, quantity, and diversity of data heavily influence the accuracy or Quality of data and capabilities of the AI model. This statement is justified by Whang in his research paper that data must be treated as a “first class citizen” in AI systems, without good data, even the best machine learning algorithms cannot perform well (Whang et al., 2021) .

2) **Algorithms** is the set of mathematical formulas and processes that enable the AI system to learn from data and make appropriate predictions or decisions to be able to output. Some of these most common algorithms include decision trees, neural networks, support vector machines, Transformers, and more. Machine learning is defined as algorithms that receive and analyze input data to predict output values, to learn and optimize their operations to improve performance” (Parsanna, 2025).

3) **Platform** , Is the hardware i use (computers, GPUs, TPUs) along with the software frameworks (TensorFlow, PyTorch, etc.) that provide the foundation to build, train, and run AI models.

Note: Beyond the CPUs and GPUs, there is another important type of chip to discuss with reference to AI . Liking the Mining Rigs in case of Blockchain technology, as the field of AI has advanced, more specialized hardware has been created, so-called the Tensor Processing Units (TPUs), originally developed by Google (Theobald, 2024).

4) **Integration** is about how the AI system is connected to and how it interacts with other systems within an organization or application (e.g., databases, user interfaces).

AI Algorithms

The field of AI is controlled & regulated by Algorithms; this is true for both Autonomous and Generative AI.

As we know, an Algorithm is a set of specific instructions designed to perform a task or solve a problem. Algorithms are the essential building blocks of a good AI system.

On a high-level different types of AI Algorithms are:

- Classification
- Regression
- Sorting
- Clustering
- Transparent & black-box Algorithms

The role of these algorithms is to perform the necessary functions to get the expected output.

Classification algorithms help categorize input data based on class. The training process involves feeding the features and class labels into algorithms. The trained model can be used to predict the likelihood. The model is actually making estimates based on trained data. The accuracy of answers is, therefore, entirely based on the Data trained and the Model.

Regression algorithms are used to predict continuous value; a linear regression algorithm could be used and trained on a data set to create a model.

A model trained on specific data can thus offer information related to health topics. The model can be reinforced to use continuous learning to learn to do better.

A Sorting algorithm is used to arrange a collection of items or data points in a specific order.

Clustering in AI is an unsupervised learning technique that automatically groups similar data points into clusters based on their intrinsic patterns or similarity, without needing labeled examples , It is widely used for customer segmentation, anomaly detection (Yin et al., 2024) . An algorithm can be classified as Blackbox, with this type of pathway from input to output cannot be easily traced or explained. An example of such an algorithm could be multi-layered neural networks. Between the Input & output process, there are multiple layers of the Feed Neural network.

Data Sets

Data is an important factor in making the AI system very effective, which is solely dependent on the algorithms in use.

Data is the Fuel & brain of AI systems, without which they cannot learn & give any output.

The technology components of AI are listed below.

1. **Machine Learning (ML)** - AI that relies on models that learn from past data to predict future situations.
2. **Deep Learning (DL)** - Deep learning is in fact an extension of Machine Learning. The differentiating characteristic of Deep Learning is that the algorithm uses a neural network. The idea of neural networks comes from the fact that neural networks mimic the way the brain functions.
3. **Natural Language Processing (NLP)** - NLP is used in Modern AI to build the GAP between human communication & machine learning (rule-based modeling of human language); NLP uses statistical, machine learning, and deep learning models to break down languages into machine readable representations. This gives AI multi-lingual capabilities as Humans do; the current trend is to create local versions or multi-language models to support others like Spanish, Chinese, French, etc.
4. **Robotic Process Automation (RPA)** - This is a set of technologies used to replicate the manual interactions of human agents with visual interfaces.

Typical applications & use cases of AI are listed below.

a. AI-powered Chatbots

b. Fraud Detection

c. Robots

d. Autonomous vehicles

e. Security systems - End-Point protection using AI.

f. Predictive maintenance

There are more use cases with greater levels of adoption & acceptance by all sectors of industry, including the automotive, healthcare, & manufacturing sides. As per the Coherent Solutions trend report on AI adoption and productivity, all knowledge workers, such as accountants and managers, can be boosted by AI adoption. Some of the user cases in retail would be hyper-personalized shopping, fraud detection & inventory management, AI driving business transformation would be its capacity to do predictive maintenance & predictive analytics to forecast demand (Coherent Solutions, 2025).

It was noted that NIST CSF still falls short in large-scale, real-time data processing and dynamic optimization capabilities, so the paper on the application of Big Data technology (BDT) proposes using BDT and Machine Learning (ML) models to design a dynamic analysis and real-time response system (Li and Zhang, 2025).

2.5.3 AI Impact on Security

According to Achuthan et al. (2024), Generative AI's ability to create adaptive, predictive models offers an unparalleled opportunity to preempt cyber threats and automate defense mechanisms, but it also poses unprecedented challenges in detecting and creating sophisticated cyberattacks.

For instance, as highlighted in the report by Bitwise on Crypto use cases (2024), "AI is introducing new problems like deep-fakes, sham videos that look convincingly real. A finance worker at a multinational firm was recently tricked into paying out over $25 million to fraudsters who used deep-fake videos to pose as the company's CFO in a video conference call" (Rasmussen and Hougan, 2024).

AI tools like WormGPT and FraudGPT were being used for illegal activities, which was a major wake-up call, and it forces us to ask tough questions about the AI we are building and putting out into the world. It’s a powerful reminder that we need to find a balance between creating incredible new technologies and making sure we control it, do so in an ethical and responsible way (Simona-Nicoleta Vulpe et al., 2024) .

According to Malatji and Tolah (2024), AI has been intersecting with Cybersecurity to classify based on its use as Defensive AI , Offensive AI & Adversarial AI , while AI is used to build

defense, carry offense, and on the other hand, AI has its own flaw or vulnerability which can be exploited through the method called Data Poisoning & input manipulation(Malatji and Tolah, 2024) .

AI has revolutionized threat detection and response mechanisms in cybersecurity. Mahbooba et al. (2021) highlight the importance of explainable AI (XAI) in enhancing trust management in intrusion detection systems (Mahbooba et al., 2021). Machine learning algorithms have been widely adopted & used for all types of predictive analytics and anomaly detection in the case of threat detection systems to enhance the ability to identify and mitigate cyber threats. As per Mahbooba et al. (2021) in her study on XAI in enhancing trust management, "However, AI also introduces new risks, such as the potential for Prompt Injection, Adversarial Attacks, Data Poisoning, Model Inversion, Backdoor Attack, Reinforcement Learning Exploit, API Abuse, Shadow AI, Identity and Impersonation Attack, Model Theft, Insecure Plugin Design adversarial attacks during the learning phases, necessitating continuous monitoring and robust defense mechanisms " (Mahbooba et al., 2021). With the advent of time, AI will take more control & the power will shift to AI, so there is a need for tighter regulation requirement , as stated in the research paper that the NSA itself is using AI with big data to counter terrorism (Muhammad Mudassar Yamin et al., 2021).

As per Simona-Nicoleta Vulpe et al. (2024) in their Journal , The Frontiers Journal on 'AI & Cybersecurity' , " focuses on the dual usage and ambivalence of AI technology in relation to cybersecurity, emphasizing their potential for both protection and harm, it states that AI is significantly impacting cybersecurity, offering both benefits and challenges" (Simona-Nicoleta Vulpe et al., 2024).

Figure 2.7

Pitfalls of AI System

The above figure on pitfalls of AI System showcases the system limitations as well as privacy & ethical concerns, which range from copyright issues, deepfakes to IP violations & more

AI can be exploited during is learning phase, as per Hu et al., “Artificial Intelligence Security: Threats and Countermeasures” explicitly organize attacks over the AI lifecycle: data collection and preprocessing (sensor spoofing, scaling attacks), training (poisoning attacks), and inference (adversarial attacks), emphasizing that AI systems are “vulnerable to various security threats throughout the whole process(Hu et al., 2021)." So, “AI dramatically enhances threat detection and response (Akhtar and Tajbiul Rawol, 2024), but it can also be exploited during its learning phases (Hu et al., 2021)." There is a long list of possible AI attacks across the AI lifecycle, including both input & output types, allowing cybercriminals to launch more sophisticated attacks.

According to (Saha, 2023), Artificial intelligence (AI) is rapidly transforming the retail landscape as well. AI-powered solutions are employed for personalized customer experiences through targeted recommendations and customized marketing campaigns. Furthermore, AI

streamlines operations through predictive analytics for inventory management and optimized supply chain logistics. AI also enhances customer service through chatbots and virtual assistants, improving response times and efficiently addressing customer inquiries. AI plays a crucial role in fraud detection and loss prevention, improving security and reducing financial losses. Moreover, ensuring the accuracy and reliability of AI algorithms is crucial to avoiding biased outcomes and maintaining customer trust. Furthermore, the use of AI in sustainability initiatives, such as optimized energy consumption and reduced waste, is expected to gain prominence. Finally, the development of explainable AI (XAI) will improve transparency and address ethical concerns ("Artificial Intelligence in Retail Market," 2023). Further, it was noted that AI has had a major impact on the education sector, particularly in its administration, instruction, and learning areas, and within the context of individual learning institutions (Chen et al., 2020). AI use case were so stronger that , AI could tasks that humans are incapable of accomplishing, which can potentially elevate social productivity to a significant extent (Cheng, 2023).

A Perturbation attack in which the Attacker modifies the query to get appropriate responses to be able to understand or map the algorithm running behind such systems. Poisoning of models is more like a traditional cyberattack. If attackers breach the AI system, then either they can compromise the existing AI model with the poisoned one, or they can execute a "Man in the middle" attack to have the wrong model downloaded, while transferring learning. Model poisoning is generally done using a Backdoored Neural Network (BadNet) attack. BadNets are modified neural networks, in which the model is trained on clean and poisoned inputs (Sangwan et al., 2023 , p.166-190) .

As we know, a deepfake is synthetic media that has been digitally manipulated, often using artificial intelligence (AI), to convincingly replace a person's likeness with that of another. This has led to an increase in the prevalence of undetectable fake content. This can be done through video, audio, or even text. This technology has negative implications, allowing attackers to manipulate digital content to spread misinformation and perpetrate fraudulent activities, posing risks to cybersecurity (Lalla et al., 2022).

Deepfakes are generated using artificial intelligence software that currently utilizes a large volume of photos or recordings of the individual to simulate and produce content. Deepfakes are created using a variety of techniques, the most prominently used techniques are Deep Learning or Generative adversarial networks (GANs).

Empowerment of AI in the context of Deepfakes has led to the creation of digital content seamlessly, enabling attackers to generate undetectable fake content as discussed, as seen with the case of the Belgian digital AI artist who created realistic videos of Tom Cruise on TikTok under the account @deeptomcruise (Lalla, Mitrani, and Harned, 2022; Li and Liu, 2021).

In the Research Paper on 'Dealing with Deep Fakes' Godulla et al. (2021) illustrate the impact of Deep fakes and the need for people to investigate not believe anything you see through the wording do not just believe what you see(Godulla et al., 2021) . At the nexus of discussions on fake news, advancing AI capabilities, and interactions between humans and machines, deepfakes exist. Utilizing AI technologies, it becomes feasible to fabricate video and audio content in a manner that deceptively resembles the original, blurring the lines between truth and falsity.

As stated by Mueller et al. (2023) strategy of disinformation and wrong propaganda through deepfakes continues & the extent to which the population continues to be captured by subtle lies and deep fakes are unknown, so this is another area of concern for Cybersecurity as the Integrity is greatly impacted with such (Mueller et al., 2023) .

As shown in Figure 2.8 below, cybersecurity incidents have increased due to the rapid rise of AI-powered attacks. With the democratization of AI, there is a surge in Cyber incidents. Threat actors are deploying Autonomous AI Agents that automate keyboard work, enabling them to find vulnerabilities and scan thousands of targets in a few minutes (Tiwo et al., 2025) Further deepfakes using AI have increased to a greater extent, around 680%, which is very concerning at this moment. The time between a vulnerability being disclosed and its exploitation has shrunk significantly, to a few hours in many cases, due to AI-assisted attacks & research. It was noted that AI driven or enabled attacks have increased over time.

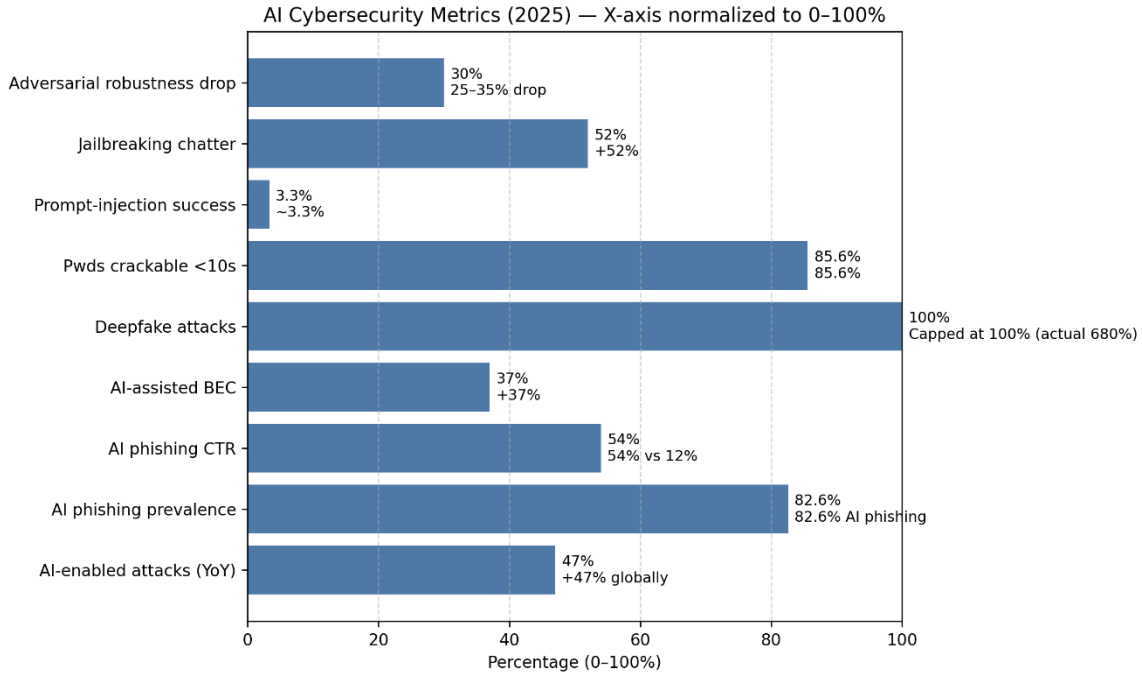


Figure 2.8

AI Cybersecurity Attack Metrics

Data source: DeepStrike (2025), The Network Installers (2025), KELA Research (2025), Zscaler ThreatLabz (2025), CrowdStrike (2025), academic adversarial-robustness studies by Yinusa & Faezipour (2025) and Villegas-Ch et al. (2024), and Deloitte's Cyber Threat Intelligence Report (2025).

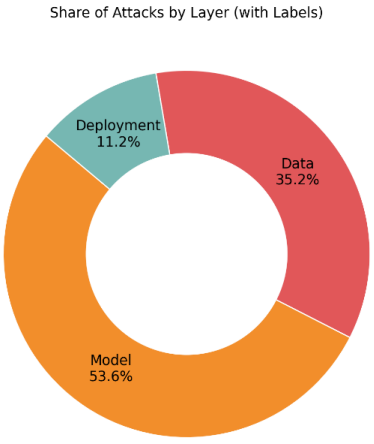


Figure 2.9

AI Attack layer-based

As per the Deep strike attack report by Hassan ,there was an Increase in the AI-assisted cyber-attacks across industries in 2025, revealed a sharp 72% increase in incidents and $30B in projected global damages (Hassan, 2025).

As shown in Figure above related to AI attack, 53% of attacks on AI target the Model itself, so there is a need to train the Model & secure it from further training-related attacks.

One of the main reasons for the rise in phishing attack success rates is the use of AI to generate deepfake videos.

AI's enhancement of traditional cybersecurity through intrusion and anomaly detection introduces unique vulnerabilities during its learning and inference phases (Sangwan et al., 2023). This is established in the research paper on 'A Review of Artificial Intelligence (AI), which states that AI revolutionizes threat detection and automation, yet remains vulnerable to manipulation, potentially allowing cybercriminals to craft more evasive and damaging attacks (Zhai et al., 2021).

The increasing use of artificial intelligence by threat actors has intensified the scale and sophistication of cyberattacks, particularly in phishing, credential compromise, and social engineering. According to the report, the AI cybersecurity sector is forecast to grow from $28.51 billion in 2025 to $136.18 billion by 2032**.** Empirical evidence indicates that AI enables rapid automation and personalization of attacks, significantly reducing detection and response windows. This shift has helped to expand the security threat surface, necessitating a more adaptive and intelligence-driven security mechanisms to maintain organizational resilience (Devasia, 2025).

As learned through the research AI's extensive use to empower technology like Deepfake, Virtual reality (VR) to Augmented reality is all adding a greater concern in the future. One consequence of these characteristics is that ChatGPT-generated interventions may be difficult to distinguish from human-generated ones; the moral benefits of ChatGPT thus remain somewhat fuzzy, and there are more clearly defined concerns (Stahl and Eke, 2024). So, there is a definite need to regulate, educate & monitor its use responsibly, which certainly talks about the need for AI Governance.

Another concern or challenge highlighted by the Forrester research on the use or adoption of GenAI is that it relies on data to generate insights unpredictably, further requiring new processes that don't exist today (Kahnke, 2024).

AI/ML-enabled dynamic risk management. As per research by High-Impact Work, AI/ML can

enhance threat detection and dynamic risk scoring but should be integrated into frameworks with explainability and governance to support decision-makers.

2.5.4 Internet of Things (IoT)

According to D.R. (2019), the Internet of Things (IoT) involves linking physical devices, vehicles, buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity. This connectivity enables these objects to gather and share data (D.R., 2019) .

International Telecommunications Union (ITU) defines IoT as a network that is available anywhere, anytime, by anything and anyone, it is also called the Internet of Everything (IOE) , this terminology IOE was coined by Cisco.

Today's IoT solutions & products come in a different range & varieties, but three main things that are general to all products are hardware, software, and connectivity.

IETF's definition of "things": In the vision of IoT, "things" are very different, such as computers, sensors, people, actuators, refrigerators, TVs, vehicles, mobile phones, clothes, food, medicines, books, etc.

These things are classified into three scopes:

1. People
2. Machines (e.g., sensor, actuator, etc.)
3. Information (e.g., clothes, food, medicine, books, etc.).

These "things" should be identified at least by one unique way of identification for the capability of addressing and communicating with each other and verifying their identities. Here, if the "thing" is identified, we call it the "object."

IEEE 2413 - IoT Framework

IEEE 2413 framework serves as a valuable tool for guiding the development, implementation, and management of IoT systems in a standardized and interoperable way. IEEE 2413 provides a comprehensive architectural framework for the Internet of Things (IoT), including descriptions of various IoT domains, definitions of IoT domain abstractions, and identification of commonalities between different IoT domains ("IEEE standard for an architectural framework for the internet of things (IoT)," 2020).

According to a research paper titled ‘Process Automation in an IoT–Fog–Cloud Ecosystem ‘, MQTT is a lightweight protocol and can be a good choice for a network protocol in an IoT application. Further, the paper concludes that Industry 5.0 will be more focused on the complete automation of the IoT ecosystem (Chegini et al., 2021).

IoT Application & its Types

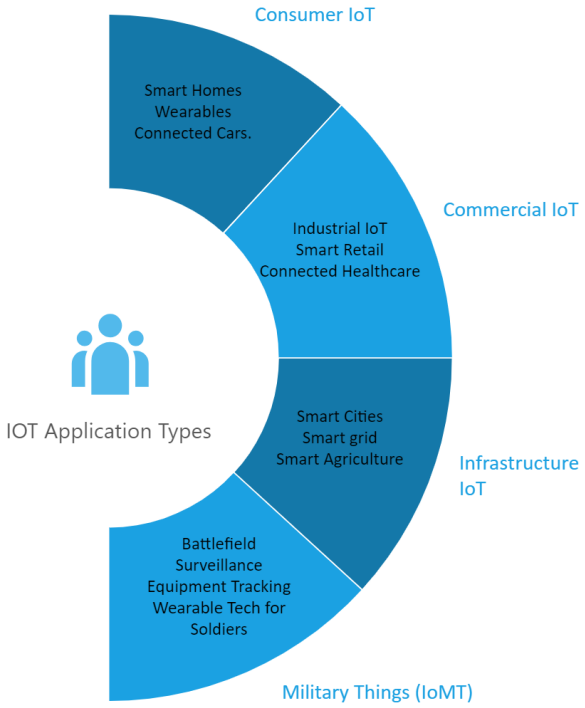


Figure 2.10
IoT Application

Infrastructure IoT can be subdivided into Critical Infrastructure IoT about National or Government & Infrastructure IoT by itself about the private sector.

Critical Infrastructure IoT pertaining to the National or Government can focus on domains like Ministry of health, waste, Agriculture, Education & Electricity. While private or public sector can focus on Smart Cities, Smart parking & more

The non-critical infrastructure IoT is also called Commercial IoT which can include intelligent transportation system, Vehicle to vehicle communication & more.

Driving Advances in IoT and M2M Communication

Four main technology areas are fueling the growth of IoT and machine-to-machine (M2M) communications:

- **Tagging Things:** Technologies like RFID, NFC, and QR codes enable unique identification and tracking of objects.
- **Sensing Things:** Sensors detect environmental changes (e.g., temperature, moisture, air quality) providing real-time data.
- **Shrinking Things:** Advances in miniaturization and embedded computing allow smaller, connected devices.
- **Thinking Things:** Devices access and process information from the web, enabling intelligent decision-making and customization (Rao, 2022) .

2.5.4 IoT impact on Security.

The wider & rapid adoption of IoT devices has expanded the attack surface, making the integration of security protocols in the design phase imperative. The paper on 'Machine learning in IoT security' discusses the challenges of rapid deployment & inherent security issues, the challenges of the heterogeneous nature of Machine-to-Machine communication in creating a 'massive attack surface', securing M2M (Machine-to-Machine) communication with constrained resources, and the need for stringent security measures creates a GAP in the environment. Another challenge is that the rapid deployment of IoT devices often outpaces the development of comprehensive security frameworks, leaving systems vulnerable to breaches and incidents (Hussain et al., 2020). Further, IEEE Std 2413-2019 , has provided an architectural framework for IoT, emphasizing interoperability and security (IEEE, 2020).

It was projected that all devices would be connected to the Internet, leading to an increase in Internet of Things (IoT) devices to around 500 billion by 2030 (Zikria et al., 2021). Furthermore, IoT devices are expected to create 79.4 zettabytes of data in the next five years, with some of this data being compact and anomalous. (Tariq et al., 2023). Despite their benefits, IoT devices, including routers and cameras, are increasingly targeted by hackers because of their inherent lack of protection due to resource limitations, leaving them permanently vulnerable (Tariq et al., 2023).

Fundamental problem is the participating nodes in IoT networks are usually resource-

constrained, making them prime targets for cyber-attacks(Hussain et al., 2020). Additionally, most of the IoT devices are manufactured with little or no consideration of their security implications (Karie et al., 2020). As per the Report by NTC Working Group from India, IoT-based solutions are increasingly utilized to create smart infrastructure across various sectors such as energy, transportation, banking, critical services, water management, smart homes, smart cities making it part of critical infrastructure (Working Group, 2023).
According to Ponemon Institute (2023) highlights that 75% of enterprises have experienced an IoT-related breach. Despite advancements in IoT devices, IoT's open research problems and future challenges stem mainly from Scalability and resource constraints.

Further as per the study by Precedence Research "The global consumer IoT market size is expected to hit around USD 616.75 billion by 2032 from valued at USD 221.74 billion in 2022 and growing at a registered CAGR of 10.77% from 2023 to 2032" (Research, 2025) **.**

Further, these IoT devices/endpoints are not easy to secure, as per Mrabet, H. et al. (2020) 'A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis', he describes how the diversity and massive number of IoT devices generate many security threats across layers, emphasizing that fast-growing numbers of networked devices and their limited resources create major security and privacy concerns.

Further, IoT connects numerous devices and drastically expands the attack surface, complicating endpoint security (Malhotra et al., 2021). Just IoT connecting numerous devices drastically expands the attack surface, complicating endpoint security.

According to Gugueoth et al. (2023) , when an attack occurs in IoT devices, all sensors and actuators associated with the device will be compromised and are to be replaced, further according to them security threats are classified on a broader sense into access control, impersonation attack (Node tampering, MITM) , Eavesdropping attack(Data Leakage, Data Theft, Data Transmit attack) , DOS & routing attack , further one of the major challenges implementing Blockchain for IoT applications as fabric lies in its heterogeneity of IoT devices , connectivity issues , its limited Power , performance & security (Gugueoth et al., 2023) .

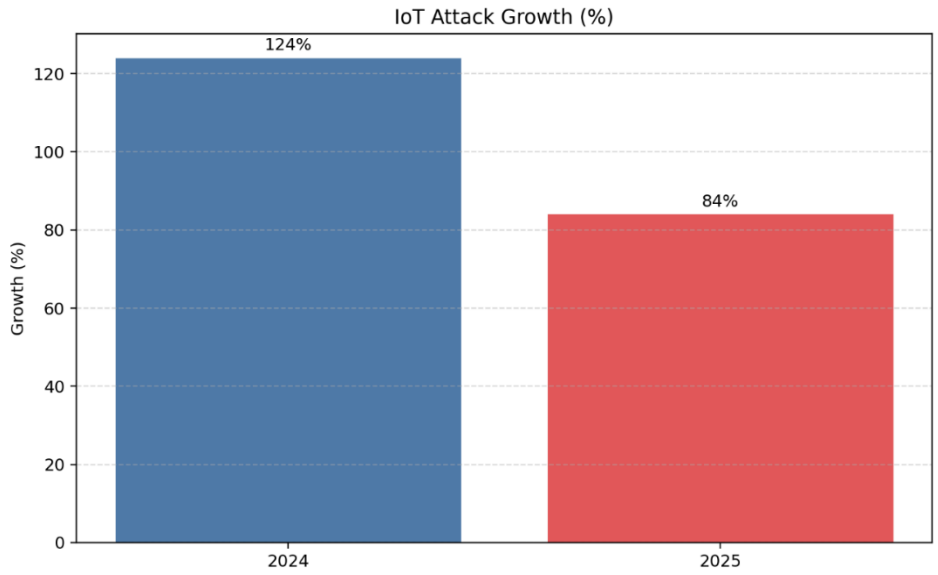


Figure 2.11

IoT Attack growth over Time , Data source: Lacoma (2025) & Bitdefender (2025) .

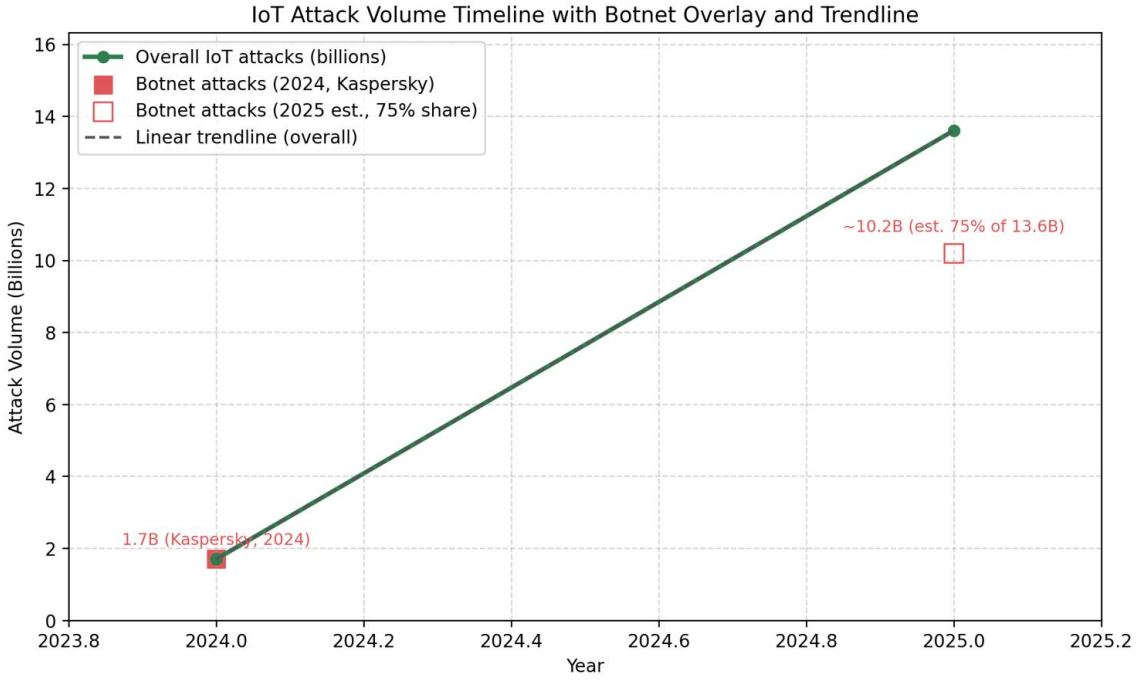


Figure 2.12

IoT Attack Volume over Time

IoT Attack Volume over Time , Data source: Kaspersky Global Research and Team (2025) , ACSMI Research (2025) & Zscaler ThreatLabz (2025).

Table 2.12

IoT Attack Growth by Year

IoT Attack Growth (2022–2025)		
Year	**Confirmed Stats**	**Source**
2022	High-growth phase; identity + IoT fraud up 1520% in IoT-heavy sectors	(Intelligence, 2025)
2023	Multi-year rise resulting in +400% IoT malware trend	(Lacoma, 2025)
2024	+124% YoY IoT attacks; +107% surge in early-2024; heavy malware increase	(SonicWall, 2024)
2025	13.6B IoT attacks; 820k per day; +84% IoT breaches; ransomware against OT/IoT +46%	(Bitdefender, 2025)

As per the IoT Attack growth table 2.12 , 2022 marked a high growth phase for IoT along with increase in Fraud , along with increased Malware in the Area , with year 2025 reported a great percentage of IoT attacks which was around 13.6 B when compared to 1.7B in 2024 , this drastic increase presents a great amount of challenge this could be due to adoption of technology like AI .

IoT increasing the attack surface, was further justified by Malhotra, P. et al. (2021) 'Internet of Things: Evolution, Concerns and Security Challenges' , the survey explains that the rapid growth and ubiquity of IoT devices, together with their resource constraints, has led to a large attack surface and significant security challenges such as DDoS and other cyber-attacks in IoT environments.

As per the Netgear IoT Security landscape report, every 24 hours, home network devices are attacked an average of 10 attacks (Team, 2024). This is an indication that IoT attacks are more prominent & are getting more popular with the increase in the IoT landscape & marketplace.

2.5.5 Blockchain Technology

In simple words, Blockchain is a Decentralized peer-to-peer distributed ledger or a digital record created by agreement among users, along with features like "smart contracts"

and other helpful tools. While a “smart contract” is a digital agreement between parties that automatically executes when specific conditions are met, parties can be a such as individuals, organizations, or automated systems, who agree to the terms and conditions encoded in the smart contract.

Each node on the Blockchain network creates & maintains a copy of this immutable ledger, typically implemented as an append-only file or a database. DLTs usually use either digital signatures or consensus to commit records. Digital records are committed to the immutable ledger as its append-only type database.

Blockchain components include nodes, which can be lightweight or full nodes. Full nodes store the entire blockchain and validate transactions. The hashing mechanism ensures the integrity of data by linking each block to the previous one through a cryptographic hash.

Blockchain provides enhanced security and transparency compared to centralized systems. It eliminates the need for a central authority, reducing the risk of single points of failure.

Implementation considerations include the Policy Administration Point (PAP), which provides an interface for creating, testing, and debugging policies. The Policy Information Point (PIP) is the source of data required for policy analysis. The Policy Decision Point (PDP) makes authorization decisions based on policies (Hu, 202).

Web3.0 is a communication layer built on top of the Internet Protocol. It utilizes blockchain technology to run the next generation of the internet and is called to be decentralized, while Blockchain is the underlying technology using Smart contracts to automate and enforce agreements on the blockchain. In the field of smart contract programming, mistakes are costly and easily exploited (Antonopoulos, 2017).

Primary Components of Blockchain technology are:

1. Decentralized Network - Utilizes a network of nodes to validate and record transactions, eliminating the need for a central authority or a central server.
2. Blocks - Containers of transaction data are represented as blocks, and, cryptographically, they are linked to form an immutable ledger that secures the integrity of the data.
3. Consensus Mechanism - Establishes agreements and network nodes on transaction validity, ensuring trust and security.
4. Smart Contracts - They are self-executing contracts with terms written directly into code that automate and enforce agreements between two peers interacting without a bank or a

mediator. Smart contracts act as Escrow. Smart contracts can talk to each other; this is often called composability, or "Money LEGO". Example: A Decentralized Autonomous Organization (DAO) uses smart contracts to execute the group's will.

5. Cryptographic Hash Function - used to convert input data into a fixed-size string of characters used for securing the integrity of blocks and transactions.

Other Components of blockchain technology are:

1. **Public/Private Key Cryptography**

Employs asymmetric encryption for secure data transmission, authentication, and access control. Creates an Immutable Ledger that stores a permanent record of all transactions, preventing data alteration and ensuring transparency, enabling direct interaction between participants, and eliminating the need for intermediaries. Uses Tokenization to represent an asset or utility on the blockchain network, facilitating the creation of digital currencies and tradable assets.

Digital Signatures are used to verify the authenticity and integrity of transactions, providing non-repudiation and data assurance.

Using an elliptic curve algorithm, private and public key pairs are created (up to 256 pairs). As a user, your private key is your secret key, and each public key is a wallet.

Figure 2.13

Blockchain Technology Characteristics

2. **Shared Ledger**

The shared ledger is a database in blockchain. There is no standard format like a relational database. The blockchain shared ledger is immutable, meaning it is tamper-proof. Secondly, it is ordered. The order is on time. These Features, combined with consensus and cryptography, yield a mechanism for delivering trust, transparency, and provenance. In Hyperledger, the ledger is divided into two main components: the ledger database and the world state database. (Zand et al., 2021).

3. **Ledger database**

The ledger database is a binary file. Blocks are appended to the file. Each peer locally hosts the file.

4. **World State Database**

The world state database is unique to Hyperledger Fabric. It is a traditional database. You can plug in your database of choice. Hyperledger Fabric defaults to Level DB (Zand et al., 2021).

5. **Consensus**

Is the concept of Trust in a blockchain network; it is like a democratic vote among computers to agree on which transactions are valid and should be added to the shared ledger.

Blockchain Consensus Tradeoff - Proof of Work (PoW) & Proof of Stake (PoS)

Proof-of-Work (PoW) and Proof-of-Stake (PoS) are the two dominant consensus families in public blockchains. They mainly differ in what scarce resource grants influence: computing power in PoW vs staked capital in PoS, leading to different profiles in security, energy use, performance, and decentralization.

A systematic review of 26 papers finds PoW with the longest-chain rule still offers the strongest formal security guarantees, though PoS can match this when carefully designed and often via hybrid or augmented models(Yan, 2022). It is a Mechanism that requires nodes in the network to solve complex mathematical puzzles to validate transactions and create new blocks.

It is an energy-intensive process; PoW consumes significant computational power, making it secure but energy-intensive. So it is, Bitcoin uses PoW consensus to ensure network security and transaction validation.

Proof of Stake (PoS):

PoS validation is based on the number of coins held, rather than computational power which PoW depends upon, to validate transactions. It is energy-efficient compared to PoW, as it doesn't require miners to solve complex puzzles. Ethereum is transitioning from PoW to PoS to reduce energy consumption and improve scalability.

Typical PoS vulnerabilities include nothing-at-stake, long-range, stake centralization; mitigations include slashing, capped coin age, and finality gadgets (Akbar et al., 2021). To note, both PoW and PoS are conceptually vulnerable to 51%/majority control, but the cost structures differ (hash power vs. stake acquisition).

Smart Contracts:

It is Self-Executing Code, Automated contracts that execute predefined conditions when specified criteria are met. It offered Decentralized Automation by operating on a blockchain, enabling trustless, secure automation of agreements. Smart contracts are transaction protocols defined to execute the terms of a contract, and play a vital role in this process. They enforce strict controls and confidentiality, eliminating the need for trusted intermediaries (Hu, 2022). Each blockchain node executing a smart contract should arrive at the same result, ensuring consistency and reliability. Table 2. 1

Traditional Contract vs Smart Contract

Feature	Traditional Contract	Smart Contract
Parties Identified By	Legal Names & Signatures	Wallet Addresses (0x123...)
Enforcement	Lawyers & Court Systems	Code & Blockchain Consensus
Trust Source	Trust in the other party/law	Trust in the code logic
Anonymity	Usually requires identity verification	Usually pseudonymous (anonymous)

Table 2.13 provides the differences between a contract & a Smart Contract to highlight the importance of code & logic in Smart contracts.

Ethereum's Innovation: Ethereum pioneered smart contracts, enabling decentralized applications and programmable transactions on the blockchain.

According to the ConsenSys Diligence Smart Contract Best Practices guide, they suggest using the Smart Contract Security Verification Standards (SCSVS), which focus on Architecture, design, and threat modelling to create secure smart contracts. It suggests considering all potential threats before implementing the smart contract (ConsenSys Diligence, 2023).

Merkle Tree

A Merkle tree, was named after computer scientist Ralph Merkle, it is a cryptographic data structure used to efficiently verify the integrity and consistency of a larger dataset. It is constructed by recursively hashing pairs of nodes until a single hash, known as the Merkle root, is obtained.

This structure enables quick, secure verification of the tree's contents, making it an essential component of blockchain technology that ensures the validity of transactions and data within the network. The information is stored on an unchangeable record. In this database, each piece of information is placed in order, and each group of information is linked to the previous group using a code. Each group also includes extra details and the code of the previous group, along with a batch of information. The information is usually organized using a hash tree called a Merkle tree. Recent work shows Merkle trees remain central to blockchain scalability, privacy, and integrity, as they are used to build field-wise verifiable transactions and redactable data on public blockchains (Davies, 2024).

Understanding Forking and Chain Reorganization in Blockchain

Forking in Blockchain

Forking in a blockchain refers to the creation of parallel chains from a single blockchain. This occurrence arises when multiple validators simultaneously produce blocks, resulting in divergent chains. These distinct chains deviate from each other due to the simultaneous block generation (Imran Bashir, 2020).

Chain Reorganization

Chain reorganization involves the alteration of the prevailing longest chain in a blockchain network. This adjustment can take place when a longer chain emerges after a network split. It can also occur if a malevolent miner crafts an alternative, lengthier chain.

Attacks and Manipulation

As discussed, malicious actors can execute attacks like the nothing-at-stake attack, the long-range attack, or the selfish mining attack to induce forking and chain reorganization. Through these methods, a malicious validator aims to tamper with the blockchain by generating multiple chains or modifying the longest chain. The primary objective of such attacks is to compromise the network's integrity and security (Imran Bashir, 2020).

Channels

Each blockchain in Hyperledger Fabric is called a channel, which is a consortium of organizations collaborating to execute transactions that are related to a specific purpose (Zand et al., 2021).

To scale higher throughput, Digital Ledger technology (DLT) is used in place of Consensus. An example of DLT is Bitcoin blockchain, directed acyclic graph **(**DAG) system like IOTA's Tangle.

In Bitcoin, all transactions are stored in a shared, append-only ledger that is replicated across many nodes in a peer-to-peer network, with no central authority; transactions are grouped into blocks, cryptographically linked, and validated via a consensus algorithm (Proof of Work), making the ledger immutable, transparent, and tamper-resistant (Asante et al., 2021).

Identities

Identities in blockchain and smart contracts represent the entities involved, such as humans and machines. These identities are equipped with private and public keys for authentication and transaction authorization. In enterprise blockchains, organizations enroll identities to facilitate transactions and administration on their behalf.

Accounts

In blockchain, accounts define access rights for executing transactions, with roles assigned permissions. Identities take on roles to interact with accounts, streamlining permission management across multiple entities.

Distributed Autonomous Organization (DAO)

The Distributed Autonomous Organization (DAO) is "kind of" incorporated on the blockchain due to its heavy reliance on end-users who serve as part-owners, part-users, and part-nodes within the decentralized network. A significant feature of a DAO is that every user functions as a "worker," and their contributions, in the form of their activities or

participation, directly impact the appreciation of the DAO's value. Some argue that Bitcoin can be viewed as the ultimate DAO (Mougayar, 2015).

2.5.6 Blockchain Impact on Security

Blockchain technology is renowned for the inherent security benefits it provides through its decentralized and immutable ledger system.

Fundamentally, Blockchain doesn't provide Confidentiality, as in most public blockchains, all transaction data is public. At the same time, this can be mitigated through privacy-preserving techniques like Zero-Knowledge proofs (ZKPs). As per the article by Kuznetsov et al. (2024) , "ZKPs are cryptographic protocols that allow a prover to convince a verifier of the validity of a statement without revealing any information beyond the truth of the statement itself. They must satisfy three key properties: Completeness, Soundness, & Zero-knowledge " (Kuznetsov et al., 2024) .

Table 2.13

Seven ways to enhance confidentiality in blockchain systems.

Technique	**Description**	**Use Case Example**
Zero-Knowledge Proofs (ZKPs)	Prove a statement is true without revealing the underlying data.	**Zcash** uses ZK-SNARKs to enable shielded transactions with hidden sender, receiver, and amount.
Confidential Transactions	Hide transaction amounts using cryptographic commitments.	**Monero** uses RingCT to obscure transaction amounts and participants.
Private/Permissioned Blockchains	Restrict access and visibility to authorized participants only.	**Hyperledger Fabric** allows channel-based data sharing for enterprise confidentiality.
Secure Multi-Party Computation (SMPC)	Joint computation over private inputs without revealing them.	**Partisia Blockchain** enables privacy-preserving auctions and voting.
Homomorphic Encryption	Perform computations on encrypted data without decrypting it.	**Enigma** (MIT project) explores privacy-preserving smart contracts.
Mixing Services / CoinJoin	Combine multiple transactions to obscure fund trails.	**Wasabi Wallet** uses CoinJoin to enhance Bitcoin transaction privacy.
Trusted Execution Environments (TEEs)	Isolate sensitive computations in secure hardware environments.	**Oasis Labs** uses TEEs for confidential smart contract execution.

The table highlights the dominance of specific vulnerabilities in the Web3 ecosystem. **Access Control** accounts for over **67%** of the total lost value, while Logic Errors, Reentrancy, and Flash Loan attacks make up the majority of the remaining losses.

The best way to turn the blockchain into a private network is to restrict access to known participants and control data visibility. According to Investopedia (2025), 51% of PoW attacks occur when an entity controls over half the network's miners and alters the blockchain. In the case of proof-of-stake (PoS), this would require owning 51% of the staked cryptocurrency.

Blockchain systems enable secure data sharing while prioritizing privacy, anonymity, and accountability, without the need for intermediaries or trusted third parties. While blockchain technology is known to offer inherent security benefits with improved transparency and efficiency, it also presents its own security challenges related to complexity, integration, smart contract vulnerabilities, and scalability. Further, Blockchain is known to enhance identity management by providing a secure, decentralized way to store and verify identities, giving individuals greater control over personal information and reducing the risk of identity theft (Ram and Verma, 2024).

According to Stodt and Reich (2020), the Data Communication Module for Blockchain (DCMB) enables smart contracts to use data signatures to keep data confidential.

The impact of blockchain on cyber/information security is both positive and negative. On the positive aspect, blockchain technology is a decentralized architecture with built-in security that increases trust and transaction integrity through characteristics such as decentralization, immutability, security, transparency, and efficiency (Singh and Kim, 2019).

Decentralized Autonomous Organizations (DAOs) address the need for transparent and efficient organizational structures. DAOs are novel, scalable, and self-organizing coordination mechanisms on the blockchain. They are controlled by smart contracts, their essential operations are automated and adhere to predefined rules without human involvement (Singh and Kim, 2019). This decentralized, automated nature can improve transparency, accountability, efficiency, and governance within enterprises.

However, smart contracts, which are fundamental to DAOs, contain loopholes and vulnerabilities if they are not taken care of and managed well, which can be exploited, leading to financial and data security risks (Christidis and Devetsikiotis, 2016). Additionally, due to the nascent nature of

blockchain technology and its complex implementation, security vulnerabilities may arise if not properly managed.

Table 2.14

Blockchain Security Incidents & Losses

Date	Project / Target	Attack Type	Loss (USD)
Nov 15, 2024	Thala Labs	Logic Errors	**$25,000,000**
Nov 16, 2024	Polter Finance	Price Oracle Manipulation	**$8,700,000**
Dec 26, 2025*	Trust Wallet	Access Control	**$7,000,000**
Nov 18, 2024	Coin Poker	Access Control	**$2,000,000**
Dec 30, 2024	FEG (Feed Every Gorilla)	Lack of Input Validation	**$900,000**
Dec 10, 2024	Clober DEX	Re-entrancy	**$500,000**

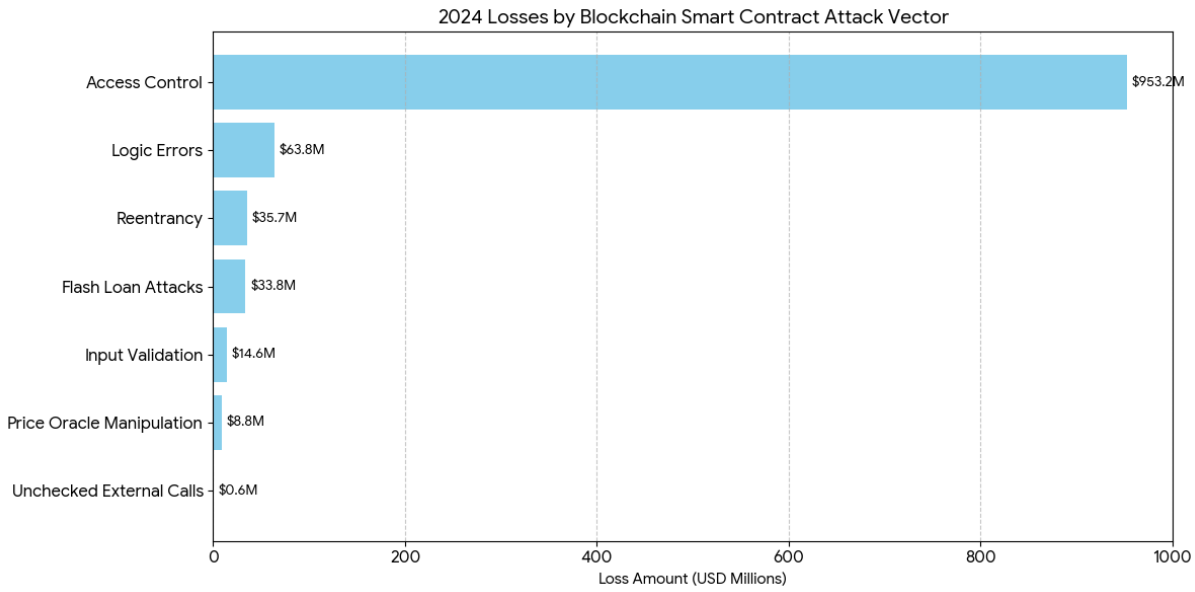


Figure 2.14

Smart contract attack vector & Losses

The bar chart above illustrates the stark differences in financial impact across various attack types. Among all the issues, **Access Control** vulnerabilities were noted to be the most damaging, accounting for over **67%** of the total value lost, responsible for nearly **$1 billion** in losses,

dwarfing all other categories like Logic Errors, Reentrancy, and Flash Loan attacks, which made up the majority of the remaining losses.

According to the research paper on, ‘A Statistical Perspective on Advancement in Blockchain Technology‘ , he states that blockchain provides system high availability to the best, as every computer in the blockchain network has a full copy of the ledger, and they all work together to keep it up to date, he states that if one computer goes down, the rest of the network continues to run smoothly due to the inherent resiliency build into such technology, It's also incredibly resilient because it can keep working correctly even if some of the computers in the network are unreliable or goes malicious.(Zhonghua and Goyal, 2022).

However, like every best solution, it also presents challenges, such as scalability, privacy, and interoperability. Komalavalli et al. (2020) discussed the security implications of smart contracts and the need for hybrid security frameworks that combine traditional methods with innovative solutions. Using Merkle trees and cryptographic signatures enhances data integrity and trust, but the complexity of blockchain systems requires careful management and governance.

Table 2.15

Key Claims & Evidence on Smart Contract issues

Claim	**Evidence Strength**	**Reasoning**	**Citations**
Smart contract vulnerabilities have caused multi-billion-dollar damages	Strong	Large surveys state smart contract bugs have incurred multibillion-dollar or huge financial losses	(Ivanov et al., 2023b)

Table 2.15 above shows that Smart Contract vulnerabilities have caused significant revenue losses. Smart Contracts have numerous bugs & issues, making them vulnerable and increasing the attack surface, exposing the blockchain system to attacks & financial losses. The above was justified by Figure 2.15, which showcases the attack vectors, and Figure 10, which shows the OWASP Top 10 data.

Several surveys and measurements show that a large share of successful blockchain attacks are rooted in smart contracts rather than the underlying consensus or network layers. “Smart contracts are prone to security vulnerabilities that have incurred multibillion-dollar damages over

the past decade, making their protection a primary challenge for blockchain ecosystems (Ivanov et al., 2023a). ” . Recent surveys emphasize that vulnerabilities in smart contracts have already caused multi-billion-dollar financial losses, indicating that the smart contract layer has become one of the most critical points of failure in blockchain systems (Chu et al., 2023).

Technically, when we talk about Blockchain security, it's good to focus on Smart Contracts, which is where all negotiations happen.

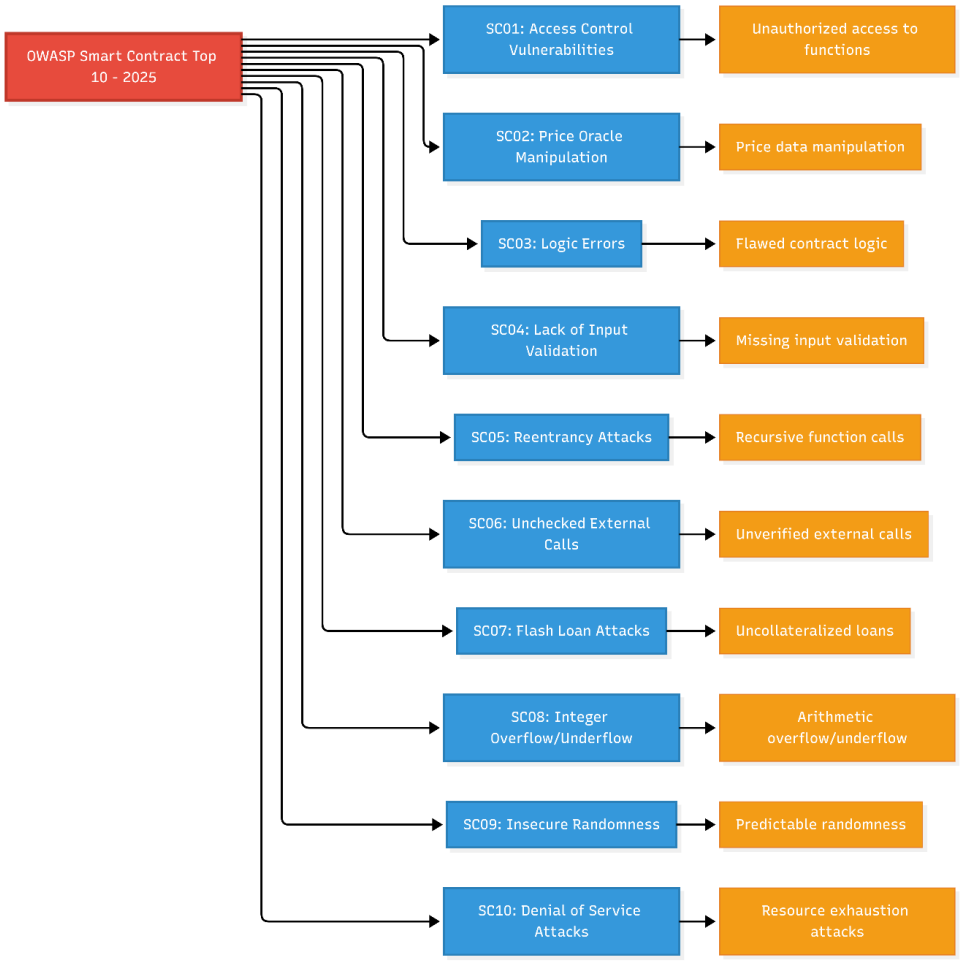


Figure 2.15

Smart Contract Top 10 Vulnerabilities, Data source: OWASP (2025).

As per the Figure-10 illustration on top-10 vulnerabilities around Smart contracts , they inherit many web-style OWASP risks (access control, injection, logic flaws) but are amplified by immutability and public visibility of code and state, Core problems include coding errors, logic

mistakes, and misuse of platform features, which are hard to patch once deployed and often lead to large, irreversible financial losses (Chu et al., 2023; Sayeed et al., 2020).

Compliance and Regulatory Challenges

Integrating emerging technologies into enterprise systems necessitates adherence to regulatory requirements and ethical standards. National Institute of Standards and Technology (2024), "Cybersecurity Framework (CSF) 2.0 provides necessary guidelines for managing and mitigating cybersecurity risks by carrying out the Cybersecurity Maturity assessment to be able to implement the required cybersecurity measures & controls or safeguards to defend the organization from evolving threats. Emerging technology risks refers to the cybersecurity related challenges that arise due to merging or integration of newer technology which are disruptive in nature so called the emerging technology, the 'Govern' Function is key to Monitoring & managing emerging risks, it calls for proactive risk management over a reactive method" (NIST, 2024) . CSF 2.0 has a greater focus on managing supply chain risks as the modern technology is heavily reliant on the complex chains which are in many cases very rigid & opaque it also as focus on Continuous improvement & its adaptability due to the dynamic nature of today's technology. CSF Protect function addresses the massive risks related to the proliferation of IoT devices & the necessity to address that. It also facilitates the integration of more specific guidance, such as the NIST AI Risk Management Framework (AI RMF), ensuring that organizations stay secure by maintaining a robust security posture and adhering to legal and ethical standards (NIST, 2024).

2.7 Proactive Risk Management Framework and Governance Model

As per Melaku (2023), in the research on Context-Based and Adaptive Cybersecurity Risk Management Framework, proactive risk management focuses on prevention by systematically identifying, assessing, and prioritizing security risks, and implementing appropriate controls to mitigate them (Melaku, 2023). Continuous learning should be incorporated to ensure the system is intelligent enough to prevent.

Organizations need to adopt adaptive governance, which involves reflecting and adapting to newer frameworks as trends and regulatory requirements evolve. Forward-thinking is crucial for organizations that call upon proactive risk management, such as addressing the challenges posed by emerging technologies.

Mızrak (2023) in his study on 'Integrating cybersecurity risk ', highlights the need & the

importance of integrating cybersecurity risk management into strategic management (Mızrak, 2023). According to Deloitte's article on 'risk management & governance' from Aggarwal, Sulabh Soral and Stubbs (2025) , "he highlights the importance of guardrails & diverse training data along with the need for human quotient, the shift in risk includes incorporating ethical guardrails, diverse training datasets, and human-in-the-loop review processes" (Aggarwal et al., 2025).The same was required in the case of risk processes, as explained by Ioannidis et al. (2023): a human-in-the-loop control mechanism was needed as a final backstop to ensure accuracy and mitigate risk (Ioannidis et al., 2023).

Governance frameworks, such as COBIT, provide guidelines for evaluating, directing, and monitoring IT management activities (Anoruo, 2019). As per Mızrak (2023) , “Continuous improvement and adaptive strategies are essential for addressing the dynamic and evolving threat landscape “(Mızrak, 2023).

According to the IDC Whitepaper from IBM, Regulatory excellence for AI comes through the digital collaboration across an organization and by using leading-edge tools and technologies that can help organizations to adopt a proactive impact assessment approach, achieved by shifting from a reactive AI compliance strategy to the proactive development of mature, responsible AI capabilities, ultimately leading to a better AI Governance model (Jyoti, 2023).

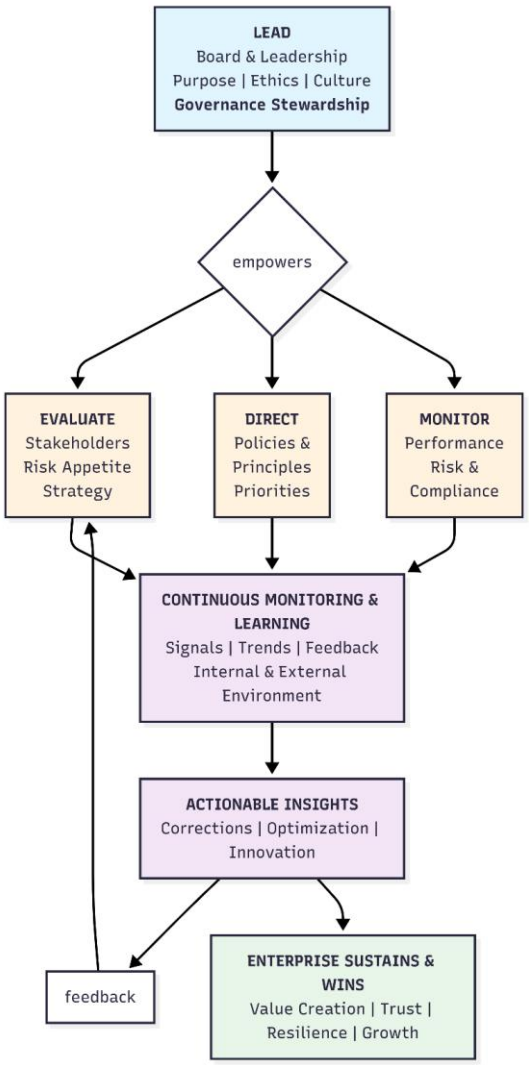


Figure 2.16

Proactive Governance Model

Figure 2.16 above provides a different perspective for Governance when compared to the COBIT framework, as per the COBIT framework “LEAD” is not explicitly mentioned as a Governance function, as per COBIT, Governance focusses on evaluation, direction & monitoring as a function, in this model we are recommending to use Lead as a driver/catalyst for the Governance function as it helps in empowering all other functions so practically its primarily an associated function of Governance, practically when we looks into this, a manager is not necessarily a Leader always, but a leader is always a good manager, A leader doesn’t just think about Outcomes, he puts himself practically into each person's position & takes measures that are driven by qualities like empathy & excellence. A leader works for others; he drives & directs

others to be leaders as well. Further, Continuous Monitoring, learning, and feedback should be part of proactive governance, so that things are handled in real time rather than reactively.

Security Architectures & Principles for a proactive SMART framework.

Zero-Trust Core is a zero-trust mindset that creates a strong foundation of control and continuous verification.

Défense-in-Depth (DID) strategic layers remain vital to ensure protection across all layers.

Movable Threat Defense (MTD) integration helps disrupt attack patterns, particularly against AI-based threats.

Security-by-design, Privacy-by-Design, and Security-by-default principles are about integrating security considerations into the design and development of systems and processes from the beginning and building privacy into systems and processes by default, minimizing data collection and maximizing user control.

As per the Gartner Article, AI trust, risk, and Information security management (AI TRISM) is a great example of human-centric security and privacy. It ensures AI model governance, trustworthiness, fairness, reliability, robustness, efficacy, and data protection. Further, the 4 pillars of AI TRISM are Privacy, AI Application Security, Model Ops & Model monitoring (Lori Perri, 2023). It is very important to ensure that the AI application is secure, that AI Sec-ops is defined & in use, and that monitoring is clear, and metrics are defined for such a model.

2.8 Cybersecurity Leadership and Organizational Culture

According to research on 'Leadership, Culture & Cybersecurity' by Safitra, Triplett & Loonam, "Cybersecurity leadership and organizational culture should enable enterprise resilience in the increasingly digital, dynamic and turbulent environments. Cybersecurity is framed as a sociotechnical and strategic issue where leadership, accountability, and innovation must be integrated with technical capabilities to build cyber-resilient organizations, strategy should be supported by culture until it becomes difficult to build cyber resilience in the organization " (Safitra et al., 2023; Triplett, 2022; Loonam et al., 2020).

The Systematic reviews on digital transformation and cybersecurity argue that emerging technologies (AI, big data, cloud, blockchain) simultaneously improve efficiency while expanding the attack surface, making cybersecurity leadership and culture central to any resilience strategy (Saeed et al., 2023; García Pérez et al., 2022). These reviews propose staged

readiness and governance frameworks in which executive commitment, clear accountability, and a security-aware culture are foundational components (Saeed et al., 2023; Annarelli et al., 2020). Organizational information and cybersecurity culture have been empirically defined as a set of shared values and behaviors characterized by an aware and knowledgeable workforce that conscientiously complies with policies "as guided by management," achieving mutual trust and integrity in information protection (Uchendu et al., 2021; Sutton & Tompson, 2024; Zanke et al., 2024). Further, the work consolidates internal and external cultural factors and highlights leadership guidance and top management support as critical drivers of the "ideal" security culture; without management support, the culture can never be built (Uchendu et al., 2021; Sutton & Tompson, 2024).

According to Lewallen (2020), Cybersecurity can be viewed as a policy challenge or a collection of interconnected policy challenges. These challenges evolve and broaden in scope in response to technological advancements that create new vulnerabilities or bring new users, objects, and interests into contact with existing vulnerabilities. New technology must be integrated to continuously develop new policies, strategies, and countermeasures (Lewallen, 2020).

The above statement can be justified through the study on emerging technology challenges; according to the research study, a greater number of studies have been carried out separately to examine the challenges from various angles without reflecting the chronological growth of this technology and security aspects to achieve better strategies to address the issues (Mogadem et al., 2021). Further practice-oriented studies have shown how leaders can operationalize cybersecurity culture through focused interventions: identifying key security behaviors, building cyber champion networks, branding the cyber team, creating security hubs, and aligning awareness with broader campaigns. These leadership-backed initiatives move organizations beyond minimal compliance toward functional cybersecurity cultures in which secure behavior is normalized and socially reinforced (Alshaikh, 2020).

Table 2.16

ET Gaps, Constraint & Challenge

Gap Category	Strategic Metric	Critical Constraint	Implementation Hurdle
AI Expertise	48% lack sufficient staff.	Rapid evolution of LLMs and agents.	High cost of specialized training.
IoT Security	12% Mature in Machine Trust.	Resource-constrained devices.	Patching inaccessible remote nodes.
Awareness	56% lack security awareness.	Sophistication of deepfake phishing.	Static, non-adaptive training modules.
Talent Growth	8% increase in skills gap.	Trailing education systems.	Lack of standardized AI security certs.

As observed in the table above, the rapid evolution of LLMs and agents leaves staff less aware of the technology & its operation, with IoT facing major constraints in implementing best security practices due to resource constraints, making it very challenging, along with other issues with references to patching for such devices makes it more vulnerable among the three Technologies in scope of this research. The table doesn't discuss Blockchain, but it presents its own integration challenges. Even though it provides a superior level of security, as we learnt, it still suffers from Smart Contract-related vulnerabilities if not properly designed & implemented in a Public Blockchain system.

The Risk Gap Matrix table below was derived from the literature review. It shows that Framework scalability from existing frameworks/regulatory is one of the primary challenges/high risks, apart from Tech Vulnerability, Integration & cultural issues. All these can be part of a Proactive framework & program that can drive them throughout the lifecycle of activities.

Table 2.17

Cybersecurity Risk-Gap matrix.

Table: Research Gap Matrix					
Research Gap	**Leadership & Human Factors**	**Technology / AI Integration**	**Regulatory / Frameworks**	**Data Protection & Governance**	**Organizational Culture**
1. Insufficient future-focused leadership models	**High - Strategic Blind Spots**	Medium - Slow Tech Alignment	Medium - Framework Gaps	Low	**High - Cultural Lag**
2. Limited preparedness and upskilling programs	**High - Skills Shortage**	Medium - Tech Adoption Risk	Low	Low	**High - Change Resistance**
3. Framework scalability and adaptability challenges	Medium - Leadership Bottleneck	**High - Integration Risk**	**High - Compliance Lag**	Medium - Partial Controls	Medium - Adaptation Issues
4. Underutilization of human factors and culture	**High - Human Error**	Low	Low	Low	**High - Awareness Gap**
5. Gaps in data protection and technology governance	Medium - Oversight Risk	**High - Tech Vulnerability**	Medium - Regulatory Uncertainty	**High - Exposure Risk**	Medium - Process Weakness

Ethical Implications and Privacy Concerns

The rapid adoption & deployment of emerging technologies raise significant ethical and privacy concerns because their use is not properly governed. For example, deepfakes using AI pose risks to data integrity and trust. Godulla et al. (2021) “discuss the impact of deepfakes on information security and the need for robust verification mechanisms. The ethical implications of AI, such as bias in responses and the inherent transparency issues, must be addressed to ensure that these technologies are used responsibly and ethically” (Godulla et al., 2021). The most crucial challenge with technology like AI is its responsible use, which is always governed by ethical

principles. While IoT, with its inherent hardware limitations, can pose significant privacy concerns, it can also be a major concern when we talk about privacy.

2.9 Impact of Geopolitical Conflicts on Cybersecurity

Geopolitical conflicts always have a significant impact on cybersecurity strategies and risk management, as they can open the door to cyber warfare. Cyberwar is one of the most prominent aspects that can occur before or during a geopolitical conflict. Sponsored groups with cyber expertise carry out coordinated attacks to obtain national secrets or cause harm to national critical infrastructure. As per Mueller et al.'s (2023) & his research on cyber operations, the Russo-Ukrainian War definitely demonstrated the complexities of managing cybersecurity in the context of geopolitical tensions, as a learning from past, organizations must be ready by developing strategies to address the risks posed by such Geo conflicts, ensuring the resilience and security of their information assets (Mueller et al., 2023). Cyber intelligence targeting a nation's critical infrastructure is a major concern worldwide, as it must always be protected in the event of a targeted strike. Hacking into infrastructure can help gain an advantage against it.

Recent reviews and empirical studies consistently identify gaps in existing enterprise-ready frameworks that assess both the strategic impact and the independent and integrated risk profile of AI, IoT, and blockchain deployments. Existing enterprise architecture and risk governance approaches (e.g., TOGAF based EA or generic cybersecurity frameworks like NIST CFS , COBIT) provide only partial, largely conceptual guidance and are not yet fully adapted to the dynamicity , socio-technical, and cross-technology nature of these systems (Alghamdi, 2024; Yaacob et al., 2023; Fuchs et al., 2025; Linkov et al., 2018).Industry 4.0/5.0 reviews and SME studies show that implementation risks span beyond technical and financial to strategic, operational, and socio-cultural dimensions, with cybersecurity and technological obsolescence among the most critical concerns (Tamvada et al., 2022; Fuchs et al., 2025).

It is important to ensure all National critical infrastructure are protected against cyber-attacks through appropriate Security Governance & proactive frameworks, as learnt through the past & present cyber-attacks that opposition’s always try to find & use the flaws in system, find vulnerabilities in those systems to exploit the system to gather required intelligence before they plot an real attack on enemy, could be an exploit on Public IP based camera’s used for Public Safety & Crime Prevention & all critical national infrastructure driven by technology with IP controller’s based SMART power grid management, IP based Supervisory Control and Data

Acquisition (SCADA), SMART Cities & other systems. As per Fang et al. (2012), security and privacy issues in the Smart Grid are major concerns that need to be addressed. So, a good Unified Proactive integrated Cybersecurity Framework that leverages best security practices, such as privacy by design for Public IP Cameras, security by default, security by design, zero trust, etc., would help nations defend against sponsored cyberattacks and crimes.

2.10 Summary

Overall, this section of the literature review suggests a clear need for adaptive, integrated hybrid proactive frameworks and strategies that enable enterprises to exploit the benefits of AI, IoT, and blockchain while proactively managing the combined or additional risks introduced by their integration. Proposed directions will include reference architectures and multi-layer hybrid frameworks for AI, IoT & blockchain systems, as well as domain-specific data governance models.

Overall, the literature review lays the foundation for enterprises to deepen their exploration of how to effectively and securely adopt AI, IoT, and Blockchain in enterprise environments. It not only underscores but also provides the importance of developing better leadership strategies and proactive frameworks that not only leverage the advantages of these technologies but also are flexible enough to proactively address the potential risks and challenges they present when adopted abruptly without a proper risk assessment and plan to integrate such technology into the existing scope.

The need for a new Hybrid Integrated Framework - No single strategy is a bulletproof solution for the vastness of emerging technology concerns. We'd greatly benefit from a more flexible, hybrid, proactive framework that can combine the security offerings from the different models & principles discussed in the Literature review section.

The figure below, from the Hybrid Integrated Framework, shows that Enterprise cybersecurity resilience emerges only when all three operate together. The intersection of all three framework domains (Governance & Risk Frameworks, Technology-Specific Security Frameworks & Proactive & Resilience-Oriented Frameworks) represents an integrated hybrid cybersecurity approach, enabling the secure adoption of emerging technologies while strengthening enterprise cyber resilience.

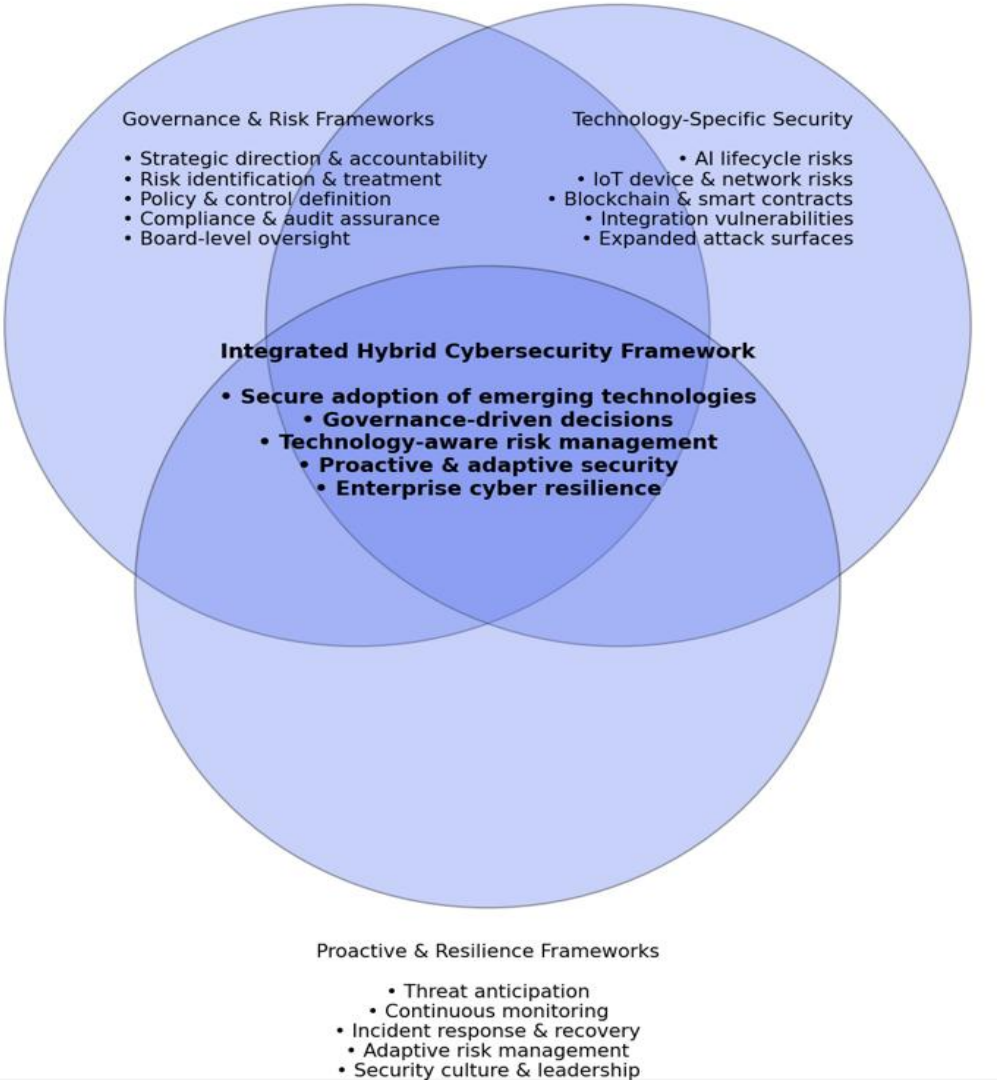


Figure 2.17

Hybrid Integrated Framework

Fundamentally, the Governance and risk frameworks are designed to provide enterprise-level direction, accountability, and compliance through well-defined Monitoring metrics, yet they remain largely static in the face of rapidly evolving technologies. While Technology-specific frameworks address AI, IoT, and blockchain risks in depth, they remain fragmented and insufficient when applied in isolation to those technologies. While proactive and resilience-oriented frameworks introduce adaptability, learning, and recovery capabilities, they require strong governance and technical grounding. So, in summary, enterprise cybersecurity resilience

is achieved not through technology adoption or governance alone, but through their mediation via proactive, adaptive cybersecurity frameworks.

CHAPTER 3

METHODOLOGY

3.1 Introduction

Enterprises adopting emerging technologies, specifically Artificial Intelligence (AI), the Internet of Things (IoT), and Blockchain, face significantly increased cybersecurity risks due to the lack of a plan and integrated, comprehensive security strategies & frameworks. Frameworks for proper risk assessment, along with a detailed integration plan, would minimize risks to some extent. Having such a deficiency leaves organizations inadequately prepared to address the unique vulnerabilities presented by these technologies and effectively mitigate evolving cyber threats in a rapidly digitizing landscape.

The primary objective of this study is to enhance understanding of how emerging technology affects information security and the measures, frameworks, and strategies that might help address the crises or gaps created by such newer technological adoption. To understand this, the study employs mixed methods to examine the impact of technology on information security. Its key goals include determining how emerging technologies pinpoint opportunities and analyzing the evolution of emerging threats and vulnerabilities, so that these technologies not only reshape but also transform information security.

Further, it focuses on identifying opportunities and threats posed by emerging technologies, thoroughly analyzing evolving threats and vulnerabilities, identifying gaps in business trinities, creating and providing a necessary framework and recommendations for addressing them, and focusing on making these technologies positively reshape and transform the IT security landscape. Ultimately, this research is aimed at helping enterprises with the necessary knowledge, best practices, leadership strategies, and tools to navigate the complexities of adopting new technology without compromising their enterprise security posture, while creating newer hybrid integrated frameworks & proactive leadership strategies to implement the required safeguards to manage risk and protect their valuable information assets effectively, to be able to maximize the benefits of such technological adoption.

Research Questions

The study is guided by the following research questions:

RQ1: What would be the security implications and strategic decision-making challenges that an

enterprise faces when adopting emerging technologies?

RQ2: What are the vulnerabilities and risks associated with integrating AI, IoT, and Blockchain technologies into enterprise systems, and how can these be mitigated?

RQ3: How does digital leadership from the information security front influence the adoption of emerging or evolving technologies, helping to secure their implementation in enterprises?

RQ4: What are the deficiencies in the available frameworks? What are the ingredients of a proactive cybersecurity framework?

RQ5: What policy frameworks and strategies based on industry best practices can be developed to enhance security while deploying emerging technologies in enterprises?

Overview of the Chapter

This chapter applies mixed-method research. It describes the research design, the population and sampling approach, the data collection and analysis procedures, and the ethical considerations guiding the study. It also presents the limitations associated with the selected research methods. Through this holistic structure, the chapter establishes a foundation for examining the relationships between emerging technology adoption, vulnerabilities, leadership influence, enterprise readiness, and the robustness of cybersecurity frameworks.

3.2 Research Methods and Design(s)

The chosen research design is a mixed–methods approach combining qualitative and quantitative research. The study begins with the LR and Case Study to understand the problem in depth, then uses those insights to develop a Survey to test whether the findings apply to a wider population. A correlational design helps identify relationships and supports the exploration and quantification of the relationships between emerging technologies and information security risks.

The specific design adopted for this research is correlational & Triangulation, which helps identify relationships and quantify them between emerging technologies and information security risks. A correlational design allows us to examine how variables—such as the adoption of specific emerging technologies can impact the incidence of cybersecurity breaches. This is essential in understanding the extent to which emerging technologies contribute to or mitigate security challenges in enterprises. Further, a Statistical Analysis is used to analyze survey data. This design will facilitate the use of correlation and regression analyses to identify patterns,

trends, and significant relationships among the variables, helping to develop newer strategies and frameworks.

3.2.1 Research Approach & Methodology

This study employs a Mixed-Method Research Design, utilizing Methodological Triangulation to validate findings across three distinct layers of study: a Systematic Literature Review (SLR), Case Studies, and Quantitative Surveys. The complexity of assessing emerging technology, specifically AI, IoT, and Blockchain within an enterprise information security context, demands a research design that captures both statistical breadth and contextual depth, so a mixed approach is in use.

Table 3.1

Research Method, Data Type its role.

Method	**Role in Strategy Development**	**Data Type**	**Statistical Application**
Statistical Analysis	Measures Variables & Dependencies.	Quantitative	Correlation, Regression, and Hypothesis Testing (p-values).
Literature Review	Identify Historical Gaps.	Qualitative	Meta-analysis of existing ET frameworks.
Case Study	Provides Contextual Validation.	Qualitative	Pattern matching and "Process Tracing" of specific ET breaches.
Survey Questionnaire	Captures Market Sentiment.	Quantitative	Descriptive stats (Mean/Median) and ANOVA

Triangulation demonstrates strong methodological convergence here due to the following reasons listed below:

Surveys (Quantitative findings) explain **what** relationships exist between the Variables.

Literature reviews explain **why** those relationships occur.

Case studies Analysis show **how** they manifest in practice.

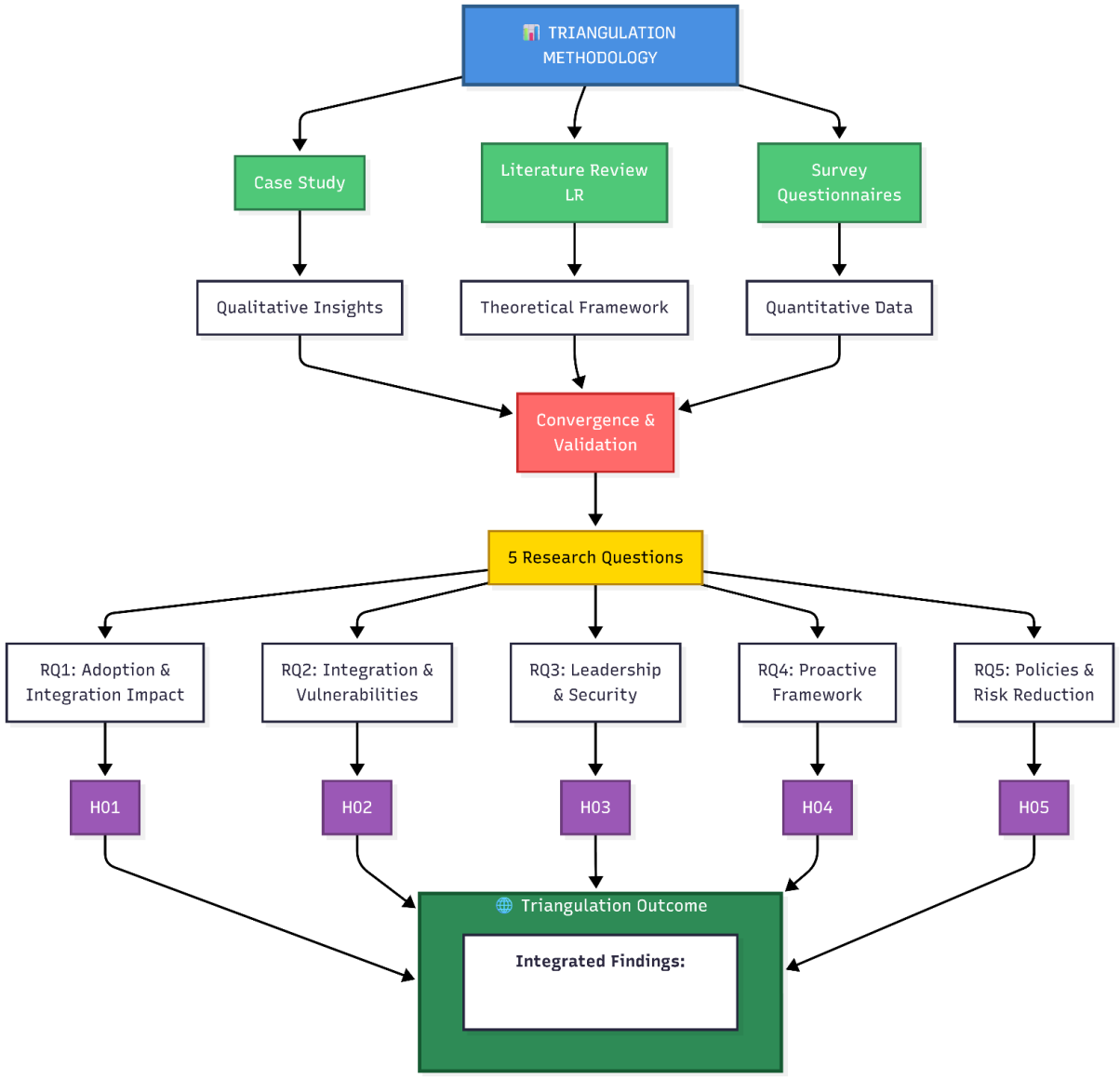


Figure 3.1

Triangulation Methodology & its Outcome

Triangulation is achieved by systematically combining **survey analysis (quantitative)**, **systematic literature review**, and **case study analysis (qualitative)**. Each method addressed the research questions from a different perspective, enabling cross-verification of results and reducing the risk of method-specific bias.

Collectively, the triangulated evidence here helps confirm the study's central conclusion.

3.2.2 Systematic Literature Review (SLR) Methodology

To ensure a highly transparent and unbiased approach to this research, the literature review will be conducted as a focused systematic review following the guidelines of the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA 2020).

The objective is to identify robust, yet relevant peer-reviewed empirical studies that explore the relationships between the specific independent and dependent variables, thereby clearly establishing the current state of knowledge and the identified research gap.

Search Strings and Keyword Mapping

The search strategy is structured around the core concepts of the research title and the variables (IVs and DVs), using Boolean operators (AND, OR) and truncation symbols (*) to maximize relevance and coverage.

Table 3.2

Search String for LR

Concept	**Search Terms (with Truncation)**
Emerging Technology (IVs 1 & 2)	"Emerging Technology" OR "Digital Transformation" OR "AI" OR "Artificial Intelligence" OR "IoT" OR "Internet of Things" OR "Blockchain"* OR "Cloud Security"
Enterprise Security (DV/Context)	"Information Security"* OR "Cybersecurity"* OR "Enterprise Security" OR "IT Security"
Impact Variables (IVs 3, 4, 5, 6,7)	"Security Breaches" OR "Vulnerability" OR "Risk Mitigation" OR "Framework Robustness" OR "Security Compliance" OR "Zero Trust" OR "Cybersecurity Investment"

Example Search String:

((AI OR IoT OR Blockchain*) AND ("Information Security" OR Cybersecurity*) AND ("Security Breaches" OR "Risk Mitigation" OR Compliance*))

Literature Eligibility Criteria

Following pre-defined criteria will be applied to all identified records to determine their relevance for inclusion .

Table 3.3

Literature Eligibility Criteria

Criteria	Inclusion	Exclusion	Rationale
Publication Type	Peer-reviewed journal articles, empirical studies, PhD dissertations, and major reports.	Opinion pieces, editorials, conference abstracts (unless complete proceedings reviewed), books.	Focus on validated, empirical evidence.
Publication Date	2018 – Present (Last 7 years).	Before 2018. Exceptions only for publications by inventors & major contributors who invented the technology or advanced it.	Ensure relevance to *Emerging* technologies and modern security practices.
Language	English language only.	Non-English language studies.	Practical constraint due to language proficiency.
Context/Population	Enterprise-level (organizational) information security, business, and management context.	Personal/Consumer security, purely theoretical computer science papers, and specific military/nation-state focused research.	Align with the enterprise focus of the proposal.
Relevance	Must empirically test or discuss the impact/relationship between at least one IV and one DV.	No direct linkage to the research variables.	Ensure direct relevance to the research questions.

Table 3.4

PRISMA Flow for Literature Selection

PRISMA Stage	Detail	Count (Target Estimate)
Phase 1: Identification		
Total Records Identified (Initial Search)	Records retrieved from all databases (Scopus, WoS, IEEE, ACM, etc.)	**4,000 - 5,500**
Records Removed before Screening (Duplicates)		**- 800 - 1,000**
Total Records for Screening	Unique records for abstract review.	**3,200 - 4,500**
Phase 2: Screening		
Records Excluded (Title/Abstract)	Records clearly non-relevant.	**- 2,700 - 3,800**
Total Records for Full-Text Retrieval	Records passing abstract screening.	**500 - 700**
Phase 3: Eligibility (Full-Text Review)		
Full-Text Reports Assessed for Eligibility	Full texts retrieved and reviewed.	**500 - 700**
Full-Text Reports Excluded	Reasons for exclusion (e.g., wrong study design, lack of empirical data, no link to IV-DV relationships).	**-950**
Total Records Included in Qualitative Synthesis	Final papers for in-depth analysis.	**100 - 150**

3.2.3 Research variables

In this study, **Independent Variables** (the cause) are the factors that we manipulate or observe, such as the Emerging technology itself & the types (AI, IoT, Blockchain) & integration levels, while **Dependent Variables** (the effect) are the measurable outcomes that are observed like the security incident frequency or framework robustness. The rationale serves as the logical bridge, justifying how changes in a specific technology or strategy are expected to directly influence the organization's security posture and resilience.

Table 3.5

Input Variable's Mapping Table

Group	Code (X)	Variable Name (as used in Results/SPSS)	Source / Item	Where Used (Models)
Emerging Technology	**X1**	Emerging Technology Adoption	"Which emerging technologies has your organization adopted? (Select all that apply)"	H_o1 (incident model)
	X2	Emerging Technology Integration Level	"How would you rate the level of integration of emerging technologies in your organization's operations?" (explicitly referenced as Integration Q15 in results narrative/models)	H_o1, H_o3, H_o4, H_o5 direct check, Overall Model
Vulnerability / Risk Exposure	**X3**	Vulnerability Index	Composite Vulnerability Index described as mean of selected indicators; item list not enumerated in the Results extract	H_o2 (predicting incident type)
Leadership	**X4**	Leadrship_index / Leadership_Index	Index used in regression outputs; item list not enumerated in the Results extract	H_o3 models; Overall Model; also used in Proactive_Framework prediction model

	X5	ET_Leadership (interaction term)	Interaction term included in Model 2 and Overall Model; construction method not stated in Results extract	H_o3 moderation test; Overall Model
Framework / Governance	**X6**	Proactive_Framework	Composite construct used as predictor of resilience; item list not enumerated in Results extract	H_o4 (key predictor), Overall Model
	X7	Policy_Framework_Strength	Composite construct used in Overall Model; item list not enumerated in Results extract	Overall Model; referenced in H_o5 mediation explanation

The table above shows the relationship between the variable input & hypothesis.

Table 3.6

Variables (X & Y)- Hypothesis Mapping Table (H_o1–H_o5)

Hypothesis	**Research Question Link**	**Independent Variable(s) (X)**	**Dependent Variable (Y)**	**Model/Test Used (as in Results)**
H_o1: Adoption & integration increase complexity leading to incidents	RQ1	X1 (ET Adoption) + X2 (Integration Level)	Y1 (Incident Frequency)	Multiple Regression (ANOVA + coefficients)
H_o2: Integration correlates with specific vulnerabilities	RQ2	X3 (Vulnerability Index)	Y2 (Incident Type)	Simple Linear Regression

H_o3: Leadership influences secure adoption and reduces breaches (tested via resilience + moderation term)	RQ3	X2 (Integration) + X4 (Leadership_Index) + X5 (ET_Leadership interaction)	Y3 (Resilience)	Hierarchical / Moderated Regression
H_o4: Proactive framework enhances resilience	RQ4	X6 (Proactive_Framework) (with X2, X4 in models)	Y3 (Resilience)	Hierarchical Regression / Model comparison
H_o5: Policies/frameworks reduce risks associated with integration	RQ5	X2 (Integration Level) (precondition check for mediation)	Y1 (Incident Frequency)	Simple Regression (direct effect check)

The above table maps both input & output variables along with Hypothesis, RQ's & the statistical method used to test relationships.

Table 3.7

X & Y Relationship table

X – Emerging Technology (Input-independent Variables)	**Y – Impact on Information Security/Cybersecurity Posture (Output - Dependent Variables)**
X1 – ET Adoption X2- Integration Level X3 - Vulnerability X4- Leadership Index X5 – Leadership & ET interaction X6- Proactive framework X7- Policy strength X=X1+X2+X3+X4+X5+X6+X7	Y1 - Incident Frequency - Outcomes Y2 - Incident Type - Outcomes Y3 – Resilience - Outcomes Y=Y1+Y2+Y3

Linear Regression Analysis:

Formula: $h(x)=\beta_0+\beta_1 x$, also represented by $y = mx+c$

Where h(x) or 'y' is the predicted value of the dependent variable (y).

X is the independent variable.

β_0 is the intercept, representing the value of y when x is 0.

β_1 is the slope, indicating how much y changes for each unit change in x.

Multiple linear regression (with more than one independent variable)

Equation 3-1: Multiple linear regression

Formula: $h(x_1,x_2,...,x_k)=\beta_0+\beta_1x_1+\beta_2x_2+...+\beta_kx_k$

$x_1,x_2,...,x_k$ are the independent variables.

β_0 is the intercept.

$\beta_1,\beta_2,...,\beta_k$ are the coefficients

Two tests under Multiple regression were carried out, one for the individual & overall.

Hypothesis test for the entire regression (F test)

H_0: if $\beta1 = \beta2 = 0$ (no Regression relationship),

H1: if at least one of the Beta quotients is not equal to zero

R2 = Coefficient of determination (% of variation in Y explained by regression)

Hypothesis for individual Parameter: β_0 & β_1 (t test)

H_0: if Beta $\beta1 = 0$

H1: if $\beta1 >$ or < 0

3.3 Population and Sample

The population will include medium- to large-sized enterprises adopting AI, IoT, or Blockchain technologies across various industries. A stratified random sampling method will ensure diverse representation across sectors, enabling a comprehensive analysis of ET adoption and its security impacts.

Targeted sample size for Survey: 1200+

Target Sample size used for Analysis: ~50 participants.

Table 3.8

Survey Instrument - Sample & Population

SI. No.	Category	Details
1	Target Enterprise Population	25 - Medium to large-sized enterprises in **Asia**
2	Key Industries	Finance, Healthcare, Retail, Manufacturing, Service sector and Telecommunications
3	Technology Focus	AI, IoT, and Blockchain
4	Target Roles	CIOs, **IT Heads**, IT Managers, and Cybersecurity Experts, Founder's , CISO , Managers & Consultants
5	Total Stakeholder Population Size (Target)	An estimated 1500+ identified professionals
6	Sampling Method	**Stratified Random Sampling** (by industry, company size, and role)
7	Target Sample (Respondent)	**~50+ Total Participants**, 2 Participants per Enterprise.

As noted in the table, the study population consists of 50+ key stakeholders from medium- to large-sized enterprises in Asia who have adopted or are in the process of adopting Artificial Intelligence (AI), the Internet of Things (IoT), and Blockchain. The enterprises in scope include those in finance, healthcare, retail, manufacturing, and telecommunications, where cybersecurity is paramount due to the reliance on digital transformation.

Table 3.9

Stakeholder Roles & Responsibilities

SI. No.	Role	Primary Responsibility in the Study Context
1	CIOs	Strategic Leadership: Defining long-term IT strategy, security policies, and investment in emerging tech.
2	IT Heads	Operational Governance: Overseeing the departmental adoption of technology and aligning IT projects with business goals.
3	IT Managers	Infrastructure Execution: Day-to-day implementation and maintenance of IT security and technical systems.

4	Cybersecurity Experts	Threat Mitigation: Managing risks, compliance, and active defense against cyber threats related to AI, IoT, and Blockchain.
5	Consultants	Assess the enterprise risk , share recommendations for mitigations.

Table 3.10

Sample Stratification Logic

S. No.	**Stratification Layer**	**Purpose**
1	By Industry	Ensures findings aren't biased toward one sector (e.g., just Finance).
2	By Company Size	Compare how SMEs vs. Large Enterprises handle security resource allocation.
3	By Role	Captures a 360-degree view from executive (CIO) to tactical (Cybersecurity Specialist & Expert).

Sample

A sample of approximately 2 participants was selected from the larger and smaller enterprises, from around 25 Larger & Medium Enterprises. The sample will use stratified random sampling to ensure representation across industries, company sizes, geographic locations, and emerging technologies within the scope of this research.

This approach allows the study to capture diverse perspectives and experiences related to the adoption and impact of AI, IoT, and Blockchain technologies. Participants from each enterprise included in the study will include key stakeholders such as Chief Information Officers (CIOs), IT managers, department heads, and cybersecurity experts, who will provide valuable insights into the challenges, strategic, and security implications of these technologies. The selected sample will help to generate reliable and generalizable findings, contributing to a comprehensive understanding of the study's purpose and objectives.

Data Collection, Processing, and Analysis

Data Collection: The date collection instruments for this study includes surveys (quantitative) and content analysis of the secondary data (qualitative - relevant literature and case

studies). The survey will be distributed to key stakeholders within the selected enterprises, including Chief Information Officers (CIOs), IT managers, and cybersecurity professionals. This targeted approach ensures that the collected data provides informed insights into technology adoption and its impact on information security.

The structured survey questionnaire is designed to gather quantitative data on the subject lines below:

• The level of AI, IoT, and Blockchain integration in enterprises.

• Perceived security issues, challenges & vulnerabilities.

• Security frameworks used or those that are currently in place to mitigate risks associated with these technologies. This targeted approach ensures that the data collected reflects informed insights regarding technology adoption and its impact on information security.

Content Analysis of Secondary Data

For each of the final included studies, the following data was extracted into a structured matrix:

- **Study ID/Citation**
- **Research Design** (e.g., Mixed-Methods)
- **Targeted Emerging Technology** (e.g., AI, IoT, Blockchain)
- **Key Finding on IV-DV Relationship** (e.g., Investment in security has a significant positive correlation with Cybersecurity Framework Robustness)
- **Gaps Identified**

This structured extraction process facilitates systematic study and synthesis, enabling the literature review module to clearly and critically assess the body of evidence, identify inconsistencies, and pinpoint the precise research gaps that this primary study should address to create a new knowledge framework or strategy.

Data Analysis: The collected data was analyzed using the available statistical software, such as SPSS. Descriptive statistics summarized the data. In contrast, correlation and regression analyses assessed the relationships between technological integration, the impact & the cybersecurity incidents and tested the stated hypotheses.

- Achieving Study Goals

This correlational design is optimal for accomplishing the study's goals for several reasons:

Empirical Evidence: The design enables the collection of empirical evidence to substantiate claims about the relationship between emerging technologies and information security. By focusing on practical & measurable outcomes, the research can provide concrete recommendations, new strategies, and frameworks grounded in data-driven insights.

Generalizability: This study's findings can be generalized to a broader context, as the sample was well defined and drawn from a specific business sector. Thus, the results are applicable to a broader range of IT enterprises planning to adopt or already facing similar challenges in adopting emerging technologies.

Focused Insight: The correlational design enables the study to focus on specific variables and their interrelationships, thereby isolating the impact of emerging technologies and security. This specificity is crucial for developing targeted frameworks and strategies that enterprises can implement to enhance their cybersecurity posture.

In conclusion, a mixed research design aligns well with the research purpose and objectives, as in the context of Emerging Technology (ET) the historical data might be lean & the threat landscape being very dynamic, so relying on a single research lens might be insufficient, so a mixed method approach a relevant, Triangulation, Contextualization, and Predictive Weighting will make the results more meaningful through a structured methodology for exploring the complex relationships between emerging technologies and information security risks. This approach addresses the study's core questions, positioning it to contribute valuable insights to cybersecurity.

3.4 Limitations

This study will have some limitations that may affect the interpretation and validity of the findings, but we are trying our best to minimize the limitations to the best by using the right sample size & right methods. Research first relies on self-reported survey data, which can introduce the risk of 'social desirability bias', where respondents may overstate their Leadership commitment or compliance to present themselves or the organization they represent in a better light. Secondly, the cross-sectional design limits causal inference, making it difficult to determine the directionality of relationships between technology adoption and associated cybersecurity risks.

Additionally, while stratified random sampling may introduce the risk that the sample does not fully represent the broader population, it also limits generalizability. Also, in statistical

analysis, the power of Regression and Correlation is influenced by the number of participants. While efforts were made to secure a diverse sample, a larger respondent pool would further enhance the "Generalizability" of the weighted framework; however, due to a limited time frame, we have used a moderate sample size. Furthermore, confounding variables, such as organizational culture and existing security measures, may influence the results if not adequately controlled. Furthermore, response bias could occur if individuals have a vested interest in technology, leading them to over-represent. Lastly, the survey measures might not fully capture the constructs of interest, affecting the accuracy of the data and conclusions drawn. These limitations will be acknowledged in the discussion of the study's findings. To overcome this, a wide range of senior staff from different business sectors has been included in this study; further case study analysis & derivation from such would help reduce bias and make this study more practical. Since the

3.5 Ethical Assurances

This research is in accordance with the ethical standards that consider privacy, confidentiality, and voluntary participation for all participants. The integrity of the research and the protection of participants' interests from risks during data collection and processing depend to some extent on the ethical standards of the research. All participant data will be kept confidential, without identifying any individual respondent. No personally identifiable information (PII) shall be collected beyond the demographics required for the statistical analysis. Using data encryption and secure storage protocols, data will be protected from unauthorized access. Based on data ownership, research will be allowed to authorized researchers, and the data will be stored on secure, password-protected servers. Before any participation, all respondents was given an information sheet about the study's aim, risks, potential controversies, and their rights as participants. The survey will be conducted on a voluntary basis. In many cases, users will have to participate implicitly by completing the survey. Participants could withdraw at any time without grounds, without being penalized or deprived of any benefits & no questions was asked. In line with the data protection rules, the study will follow the ISO/IEC 27001 security standards. As a result, the minimum requirements are secure data handling, encryption, and controlled access for research data. We will use all this data only for academic research and will not share it with any third party. Having no invasive procedures, sensitive personal questions, and experimental interventions, the study intentionally minimizes risk to participants. Strong

security measures and a well-designed survey will mitigate the risks, such as data breach or response bias.

Retained data will only be kept for a period sufficient to conclude research analysis. Raw data will be deleted in accordance with data protection best practices upon conclusion of the study and will be documented to prevent future misuse or unauthorized access.

By implementing these ethical considerations, the study ensures that all research activities are conducted responsibly, safeguarding participant rights and data integrity while maintaining transparency and accountability.

3.6 Proposed Research Framework

The Proposed Research framework helps us understand how emerging technologies affect enterprise information security, how existing and hybrid frameworks mediate these effects, and how leadership, culture, and proactive security measures moderate the resulting security outcomes. This section integrates theoretical & Conceptual constructs from the literature on the RMF, CSF 2.0, FAIR, Cyber Resilience Theory, Dynamic Risk Assessment Models, IoT, and Blockchain security frameworks, and security culture.

Core Dimensions of this Research Framework

The conceptual model is built on our five primary constructs directly linked to research questions RQ1–RQ5:

1. Emerging Technology Adoption (IV — RQ1, RQ2)

This construct captures the level and the pace of AI, IoT, and Blockchain adoption.

Each technology introduces unique vulnerabilities of its own type:

AI → adversarial AI, data poisoning, model theft

IoT → massive attack surface, endpoint insecurity

Blockchain → smart contract risks, consensus vulnerabilities

These risks drive the need for updated frameworks and secure-by-design integration strategies.

2. Technology Integration Depth (IV — RQ2)

Integration depth refers to the extent to which emerging technologies are embedded into enterprise systems, processes, and architectures.

Higher integration amplifies scaling challenges, interoperability risks, and governance gaps , a planned integration with proper testing before a production rollout would reduce some of these issues .

Traditional frameworks (RMF, CSF 2.0, ISO/IEC 27001) often cannot scale effectively without modification , because they were rigidly developed without scalability in mind . This construct explains why existing frameworks struggle with emerging technologies.

3. Cybersecurity Leadership & Culture (Moderator — RQ3)

Leadership and culture act as critical moderators across all technology-related risks as they can moderate the risks & issues by proactive measures rather than reacting.

Strong leadership → improved framework implementation, secure behavior & better compliance.

Weak leadership → policy drift, poor adoption of security controls, culture gaps due to inconsistency across people, process & practices.

This dimension reflects the research finding that technical security alone is insufficient without a proper cultural, behavioral and leadership-driven resilience.

4. Cybersecurity Framework Robustness (Mediator — RQ2, RQ4, RQ5)

This construct represents the effectiveness and adaptability (flexibility) of existing frameworks (RMF, CSF 2.0, FAIR, ISO/IEC, COBIT) when applied to emerging technologies.

A robust framework must include the below features:

a) Support lifecycle governance (Example: AI RMF)

b) Scale across IoT ecosystems (Example: NIST IR 8259)

d) Integrate blockchain-specific security (Example: consensus, cryptography, smart contracts)

d) Enable continuous monitoring and adaptive control selection.

This construct mediates the relationship between ET adoption and security outcomes.

5. Enterprise Information Security Posture (DV — RQ1–RQ5)

The dependent variable measures:

i) Security breach frequency/severity

ii) Framework effectiveness

iii) System assurance

iv) Risk mitigation success

v) Organizational resilience

All independent and moderating constructions ultimately converge here.

Conceptual Model

The proposed conceptual framework suggests a chain of effects. The initial technology adoption must lead to significant Technology Integration Depth, which, in turn, necessitates the development of deeper Cybersecurity Framework Robustness

(Mediator 1). A robust framework then enables more effective Proactive Security Measures (Mediator 2), which directly serve as the antecedents to the final Dependent Variable (DV), the Enterprise Information Security Posture.

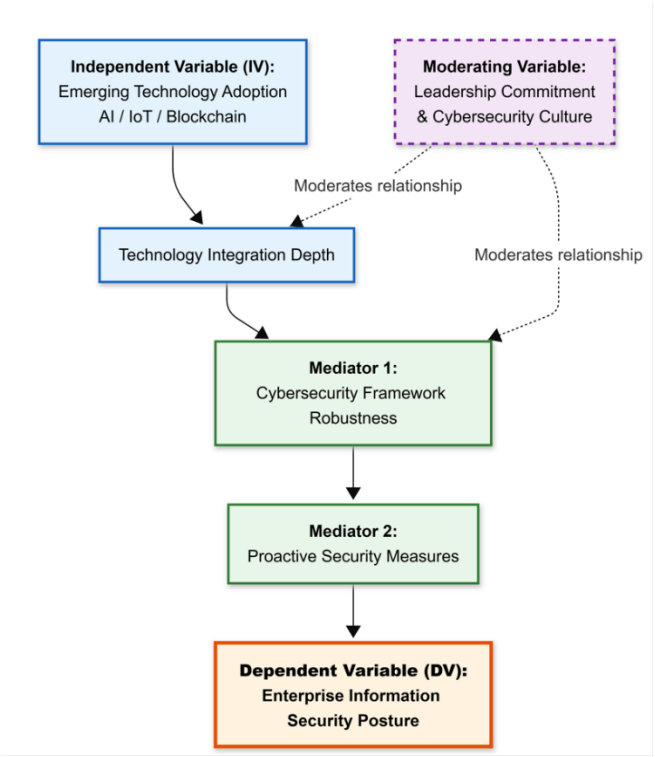


Figure 3.2

Conceptual Model Visual representation

The Conceptual Model, with a visual representation, is used to understand the relationship between all variables & its capability to influence/moderate dependent variables. Conceptual Model tried to test if Cybersecurity Resilience which is tied with Enterprise Information security Posture is affected by dept of integration, how Leadership & commitment helped with Emerging technology secure adoption, vulnerability & Incidents post adoption, policies influence on Resilience, it was noted that through the Qualitative & Case Study analysis, Integration added specific vulnerabilities but with a proper strategy, planning with a proactive

Cybersecurity Framework would help enterprises to evade many of these issues leading to a higher Cybersecurity Resilience.

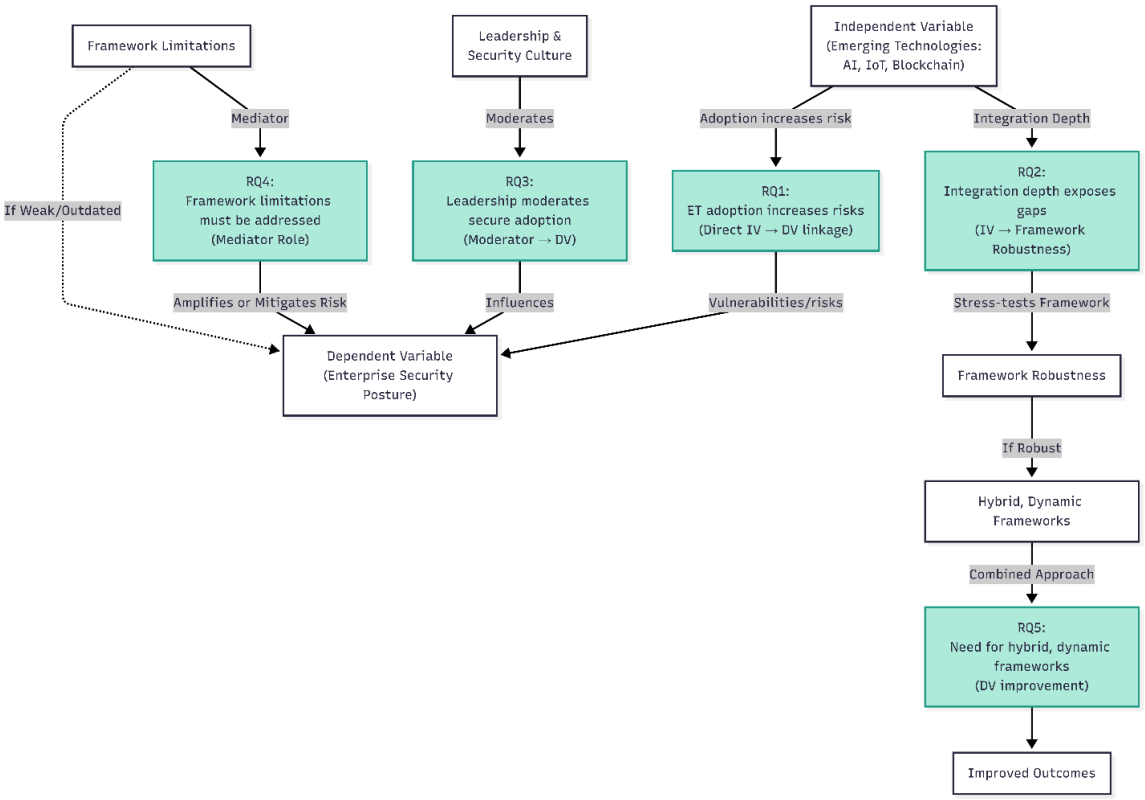


Figure 3.3

Conceptual Model and RQ's Alignment

The figure above presents the conceptual alignment between the research questions and the core variables, showing how emerging technologies directly influence enterprise information security.

RQ1 — ET adoption increases risks → Direct IV → DV linkage

AI, IoT, and Blockchain introduce vulnerabilities that affect the enterprise's security posture.

RQ2 — Integration depth exposes gaps → IV → Framework Robustness

Tightly integrated technologies stress-test the limitations of existing frameworks.

RQ3 — Leadership moderates secure adoption → Moderator → DV

Security culture and leadership influence the adoption and implementation of protective measures.

RQ4 — Framework limitations must be addressed → Mediator role

Weak or outdated frameworks amplify risk; adaptive frameworks mitigate it.

RQ5 — Need for hybrid, dynamic proactive frameworks → DV improvement

A combined approach (governance + resilience + technical controls) improves outcomes. The statistical analysis results showed that a Robust Framework, a hybrid, dynamic, Dynamic Proactive framework, delivered Cybersecurity resilience and improved enterprise security posture.

Summary of Conceptual Framework

The conceptual framework devised for this Research clearly explains why emerging technologies elevate enterprise security risk (RQ1), highlighting the integration depth and scalability gaps that challenge existing frameworks (RQ2, RQ4), while demonstrating the moderating influence of leadership and culture (RQ3), and finally, establishing the need for adaptive hybrid frameworks (RQ5)

To provide the analytical foundation for Survey instrument design, Hypothesis development, Framework evaluation & the proposed hybrid cybersecurity model presented in the later section.

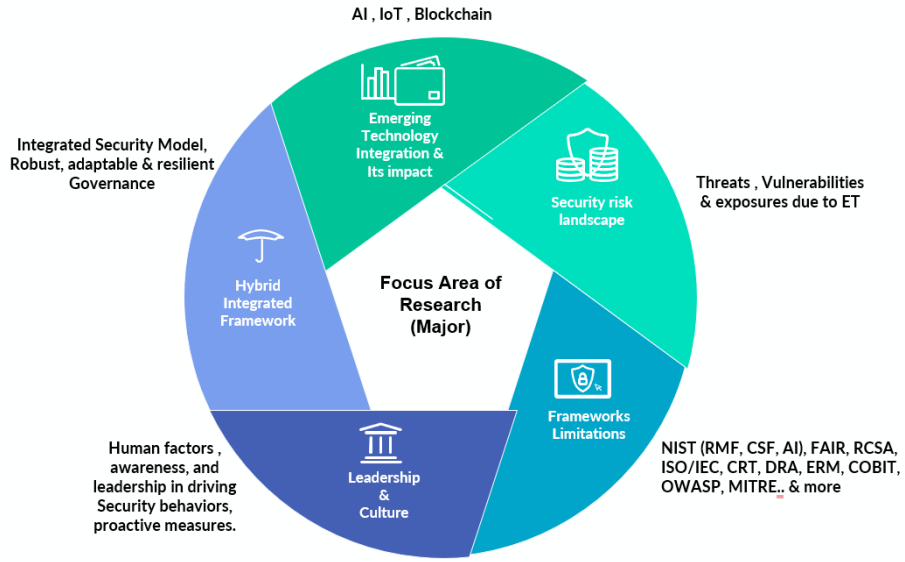


Figure 3.4

Primary Focus Area for this research

Research Model Architecture

Direct Path: Emerging Tech Adoption **(IV)** → Security Posture **(DV).**

Mediation: Adoption **(IV)** → Framework Robustness **(Mediator)** → Security Posture **(DV).**

Moderation: The strength of the relationship between Adoption and Security is changed (strengthened/weakened) by the Leadership & Culture **(Moderator)**

Table 3.11

Proposed Variable & Hypothesis Testing Matrix

Research Element	**Variable Role**	**Statistical Test**	**Purpose**	**Hypothesis Goal**
RQ1: Adoption Impact	IV: ET Adoption DV: Security Posture	Multiple Linear Regression (ANOVA + Coefficients)	Test for Independence. Does adopting ET "X" change the likelihood of a breach?	Reject H_0: Adoption and breaches are significantly associated.
RQ2: Integration Depth	IV: Integration Depth DV: Security Posture	Simple Linear Regression (ANOVA + Coefficients)	Measure the strength of the link between system "embeddedness" and risk.	Significant positive correlation ($r>0.5$) between depth and vulnerability.
RQ3: Leadership Influence	Mod: Leadership/Culture IV: ET Adoption DV: Security Posture	Moderated Regression (Interaction Test)	Determine if Leadership weakens the negative impact of tech on security.	Interaction effect: High leadership scores lower the risk slope.
RQ4: Framework Role	Med: Proactive Framework & Resilience IV: ET Adoption DV: Security Posture	Multiple Regression / Hierarchical Regression (Model comparison)	Test if ET only improves posture through a robust framework.	Indirect effect: Framework quality explains the success of the IV.
RQ5: Policy Framework & Incident Risk (H_05)	IV: Integration Level (Q15) → DV: Incidents (Q20) (mediation precondition check)	Simple Linear Regression (Direct effect check)	Check whether integration predicts incidents (required first step before mediation)	Check if the implementation of comprehensive security policies and governance frameworks significantly reduces cybersecurity incident risk

Overall Model	All IVs, Med, & Mod		To calculate the Predictive Power (R2) of the entire model.	Identify which variable is the strongest predictor of resilience.

3.7 Summary

The purpose of this study was to understand and examine how Artificial Intelligence (AI), the Internet of Things (IoT), and Blockchain will affect enterprise information security, the associated risks, the strategies used to minimize those risks, and leadership participation in cybersecurity management. We examine how these new technologies affect security and provide the resilience frameworks enterprises need to defend against evolving threats. A quantitative correlational research design was undertaken to analyze the interaction of emerging technology adoption and cyber risks. The aim of the study was to examine the empirical approach Enterprises should use to tackle security risks induced by Emerging technologies. The research was probed earlier through 5 key questions (i.e., ET & its security implications, risk factors, leadership influence, Proactive Risk Framework & policies) to deal with the issues of security implications, risk factors, leadership influence, policy framework and continuous improvement strategies.

The hypothesis was that higher security risks arise from emerging technologies and that stronger security leadership and well-established frameworks can address them. Research is aimed at key stakeholders from medium- to large-sized enterprises across the finance, healthcare, retail, and telecom industries in Asia. The players involved in technology adoption and risk management are primarily CIOs, IT managers, and cybersecurity experts. A stratified random sampling will be employed to obtain a roughly 50-person sample from 50 enterprises, thereby achieving a representative sample of industries and occupational roles.

Data was collected by giving a structured survey questionnaire with 30–35 Likert scale questions on a researcher. The question I will ask in my survey has to deal with technology adoption, security risks and how effective the existing security frameworks currently are.

The data was analyzed using statistical software programs like SPSS to describe the data and study correlation analysis as well as regression analysis to understand the relationship between emerging technology adoption and cybersecurity incidents. Other limitations include self-reported bias of the survey, response bias, and sample representativeness. Further, this cross-

sectional design may also limit inferences of causation and confounding factors, organizational culture, could have an impact on results. Some of these factors will be taken into consideration while interpreting the findings to have a balanced and objective analysis. That said, we strictly adhere to the same set of data protection measures such as GDPR or equivalent pertaining to the location where such data is collected and ISO/IEC 27001 respectively, amongst other leading practice of ethical integrity of the research. Participants' data will be anonymized and securely stored, and only authorized researchers will have access to it. Participants will be voluntarily able to participate in the study and the organization will provide an information sheet disclosing the rights of the participants, such as abstaining at any time with no consequences. A methodological approach based on generating data-driven insight into the adoption of AI, IoT, and Blockchain-related cybersecurity challenges was employed in the study. The research considers security risks, the role of leadership, and the security resilience strategic frameworks with recommendations to enterprises on how to bolster their security resilience in the evolving digital space.

CHAPTER 4

RESULTS

4.1 Introduction

The Research chapter presented the study's practical results on the impact of emerging technologies on enterprise information security. These findings are derived from the statistical analysis of survey questionnaire response data collected from professionals across multiple IT industries and organizational sizes. The study investigates how digital leadership in information security influences the adoption of emerging or evolving technologies, focused on vulnerabilities and risks associated with integrating AI, IoT, and Blockchain technologies into enterprise systems, and how these can be minimized or completely mitigated. To investigate these relationships, the study collected quantitative data from around 50 respondents. The data was analyzed using statistical tests using IBM SPSS. The results are as follows. These results are structured in alignment with the research objectives defined in this study.

4.2 Demographic Outcomes:

The findings from demographic analysis are as follows.

A total of 50 valid responses were analyzed. Among these, most respondents were in the 31–40 age group (38%), followed by 49–58 years (28%) and 41–48 years (20%). So the sample was predominantly male (88%). Educational qualifications were high: 98% of respondents held at least a bachelor's degree. Most respondents were employed full-time (84%) and held senior or decision-making roles, such as CIOs, IT Managers, CEOs, and Risk or Security Managers.

Legend for Table: Profile of Respondents and Organizations (n = 50)

Note: Percentages are based on total sample size (n = 50). Missing responses are reported as "Missing/Unspecified".

Table 4.1

Age of the respondents

Category	n	%
22–30	6	12.0
31–40	19	38.0
41–48	10	20.0
49–58	14	28.0
58 & above	1	2.0
Total	50	100.0

The table above indicates that the sample is predominantly composed of mid-career and senior professionals, thereby enhancing the credibility of responses regarding enterprise information security and emerging technologies.

Table 4.2

Gender of Respondents

Category	n	%
Male	44	88.0
Female	5	10.0
Missing/Unspecified	1	2.0
Total	50	100.0

The above Table shows that the sample predominantly consists of males, suggesting a gender imbalance that may reflect existing demographic trends in leadership and cybersecurity roles within organizations.

Table 4.3

Education level

Category	n	%
Bachelor's Degree	28	56
Master's Degree	19	38
Doctorate (Ph.D.)	2	4

Missing/Unspecified	1	2
Total	50	100

The table above shows that 98% of respondents have at least an undergraduate degree, suggesting a highly educated sample capable of understanding complex cybersecurity and technology integration issues.

Table 4.4

Current employment status

Category	**n**	**%**
Full-time	42	84
Self-Employed	4	8
Unemployed	4	8
Total	50	100

The above table shows a high proportion of full-time professionals, suggesting that most participants are actively engaged in organizational environments, making their responses relevant for analyzing enterprise-level cybersecurity practices.

Table 4.5

Sector of employment (primary work sector)

Category	**n**	**%**
Other	24	48
Finance/Banking	11	22
Telecommunications	5	10
Government/Policy	4	8
Manufacturing	4	8
Retail	1	2
Missing/Unspecified	1	2
Total	50	100

The Table data revealed sectoral diversity; a large “Other” category may require clarification for deeper, sector-specific analysis.

Table 4.6

Years of experience

Category	n	%
22+ years	11	22
5 – 8 Years	11	22
14 – 18 Years	10	20
19 – 22 Years	9	18
9 – 13 Years	8	16
Less than 4 years	1	2
Total	50	100

The table above shows that most respondents had substantial professional experience, strengthening the reliability of insights on cybersecurity leadership and technology integration.

Table 4.7

Current position in the organization

Category	n	%
IT Manager	9	18
CIO	8	16
CEO	6	12
Other	6	12
Technology Specialist	5	10
Sr. Consultant	5	10
Risk/Security/Compliance Manager	5	10
Business Development	3	6
Cybersecurity Expert	2	4
Head of Dept	1	2
Total	50	100

The table above shows that the majority of respondents hold decision-making or technical leadership roles, making the dataset highly relevant for studying cybersecurity governance and emerging technology adoption.

4.3 Organizational Characteristics

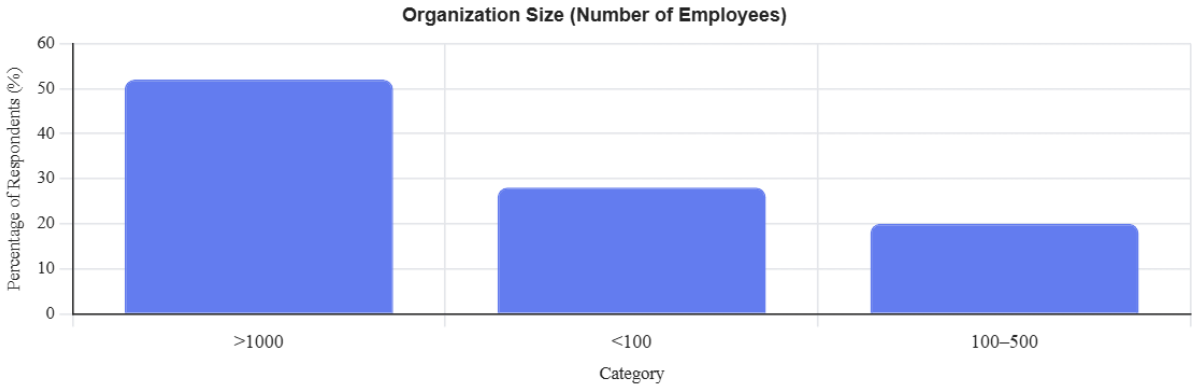


Figure 4.1 Number of employees in the organization

The sample includes both large enterprises and smaller firms, allowing comparison across organizational scales. Importantly, more than half of respondents (52%) worked at organizations with over 1,000 employees, making them larger enterprises, while the remainder worked at medium or small organizations.

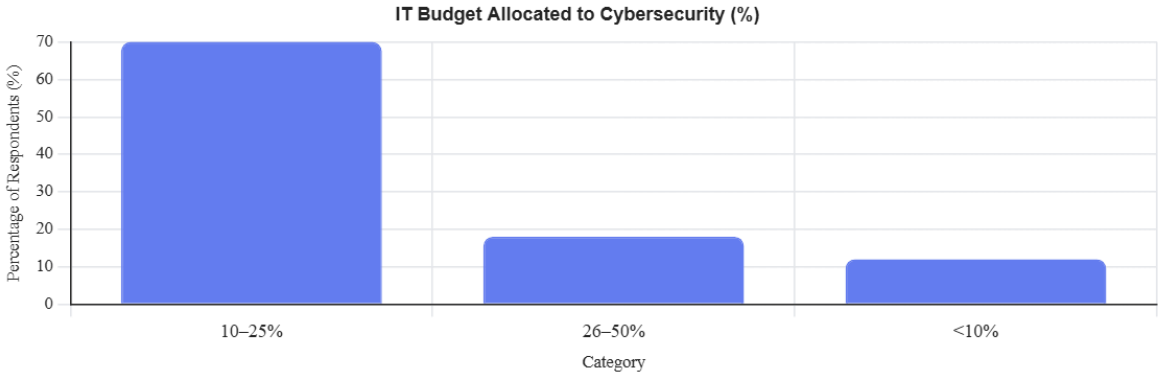


Figure 4.2
Percentage of IT budget allocated to cybersecurity

The figure above indicates that moderate cybersecurity investment levels are common across most organizations, with relatively few allocating very high budget shares.

Most organizations (70%) allocate between 10–25% of their IT budget to cybersecurity. While a smaller proportion allocated 26–50% (18%), while 12% allocated less than 10% of IT budget, suggesting moderate but not aggressive cybersecurity investment across most organizations.

Figure 4.3

Cybersecurity Incident Response

According to the bar chart above, 60% of organizations report responding to cybersecurity incidents immediately, while 30% respond within 24 hours. Only a small fraction responds within a week or rarely/never, indicating relatively strong operational incident response capabilities among respondents.

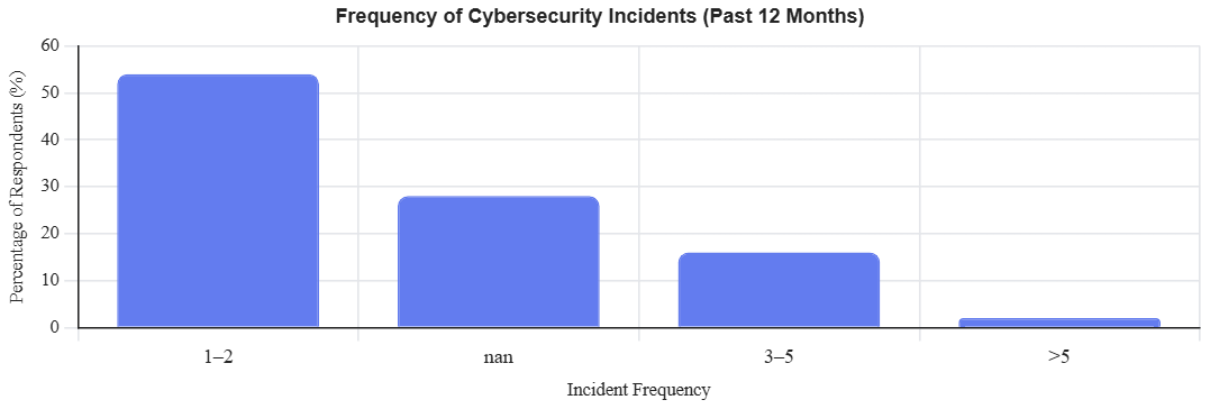


Figure 4.4

Frequency of Security Incidents (Incident Experience)

As per the above chart, 54% of organizations experienced 1–2 cybersecurity incidents in the past year, while 28% reported no incidents. Fewer organizations experienced higher incident frequencies (3–5 incidents or more), suggesting that while incidents are common, they are generally limited in number.

4.4 Results from Statistical Analysis:

Findings on RQ 1 & H_o1:

RQ 1: What would be the security implications and strategic decision-making challenges that an enterprise faces when adopting emerging technologies?

The first research question aims to examine the security implications and strategic decision-making challenges that an enterprise faces when adopting emerging technologies. The first research hypothesis that was relevant to the first research question reads:

"The adoption of AI, IoT, and Blockchain technologies increases the complexity of enterprise security management, leading to cybersecurity breaches and incidents". The findings are as follows .

Table 4.8

ANOVA for research hypothesis 1

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	7.211	2	3.605	9.175	.000[b]
	Residual	18.469	47	.393		
	Total	25.680	49			
a. Dependent Variable: How many cybersecurity incidents has your organization experienced in the past 12 months?						
b. Predictors: (Constant), How would you rate the level of integration of emerging technologies in your organization's operations? Which emerging technologies has your organization adopted? (Select all that apply)						

The table above indicates that the model is statistically significant ($F = 9.175$, $p < 0.001$), demonstrating that emerging technology adoption and integration levels jointly predict cybersecurity incidents.

Table 4.9

ANOVA for research hypothesis 1

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.909	.521		1.746	.087
	Which emerging technologies has your organization adopted? (Select all that apply)	-.185	.045	-.571	-4.136	.000
	How would you rate the level of integration of emerging technologies in your organization's operations?	.496	.175	.391	2.836	.007
a. Dependent Variable: How many cybersecurity incidents has your organization experienced in the past 12 months?						

There is a positive and substantial correlation between cybersecurity events and the degree of new technology integration ($\beta = 0.391$, $p = 0.007$). This implies that increased incident frequency is linked to higher levels of integration, most likely due to larger attack surfaces and more complex systems.

Remarkably, there is a substantial negative correlation with the technology adoption variable ($\beta = -0.571$, $p < 0.001$). This implies that, in contrast to partial or informal adoption, organizations that formally embrace emerging technology may put in place established controls that lower occurrences. This suggests that the primary risk element is integration intensity rather than adoption alone.

$H_0 1$ is only partially supported overall. When combined with governance procedures, structured technology adoption seems to reduce risk, even while the integration level raises incidents.

Findings on RQ 2 & $H_0 2$:

RQ 2: What are the vulnerabilities and risks associated with integrating AI, IoT, and blockchain technologies into enterprise systems, and how can these be mitigated?

The second research question investigated the vulnerabilities and risks associated with integrating AI, IoT, and Blockchain technologies into enterprise systems, and how these can be mitigated. The second research hypothesis states:

"Integrating emerging technology into enterprise systems significantly correlates with increased specific vulnerabilities, such as data privacy issues and scalability concerns". The findings are as follows.

Table 4.10

ANOVA for Research Question 2

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	7.735	1	7.735	6.839	.012[b]
	Residual	54.285	48	1.131		
	Total	62.020	49			
a. Dependent Variable: What was the most common type of incident?						
b. Predictors: (Constant), Vulnerability						

Table 4.11

Linear Regression Analysis for research question 2

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	4.754	.740		6.427	.000
	Vulnerability	-.467	.178	-.353	-2.615	.012
a. Dependent Variable: What was the most common type of incident?						

The findings provide H_o2 empirical backing. The integration of emerging technologies is closely linked to cybersecurity risks arising from vulnerabilities. Certain incident types may be more likely to occur in organizations that integrate modern technology without sufficiently bolstering governance and security procedures.

When incorporating new technologies into corporate systems, our findings emphasize the significance of adaptive cybersecurity frameworks, secure-by-design principles, and proactive risk assessment.

Findings on RQ 3 & H_o3:

RQ 3: How does digital leadership from the information security front influence the adoption of emerging or evolving technologies, helping to secure their implementation in enterprises?

The third research question examines how digital leadership from the information security domain influences the adoption of emerging or evolving technologies, thereby helping secure their implementation in enterprises. The third research hypothesis states:

"Strong information security leadership positively influences the secure adoption and implementation of Emerging technologies, reducing the likelihood of security breaches".

The results provide partial support for the third hypothesis. The adoption and deployment of emerging technologies are significantly improved by leadership commitment. However, rather than broad policy commitment, active leadership participation is the main factor driving the direct reduction of cybersecurity incidents.

This implies that formal regulations and resource allocation are necessary for efficient cybersecurity governance, but so is senior leadership's direct strategic involvement. There are fewer breaches in organizations when the leadership actively participates in cybersecurity decision-making, underscoring the significance of executive-level responsibility in business information security. For more information on statistical data & Analysis, refer to Table 7.5 - Appendix B.5: ANOVA for RQ 3 & Table 7.6 -Appendix B.6: Moderated Regression (Interactive test) Analysis for RQ 3

Findings on RQ 4 & H_o4:

RQ 4: What are the deficiencies in the available framework? What are the ingredients of a proactive cybersecurity framework?

The fourth research question investigates deficiencies in the available framework and the ingredients of a proactive cybersecurity framework.

The fourth research hypothesis states that “a proactive cybersecurity framework may combine risk-driven strategy, strong culture and governance, and advanced technical controls with resilience and user-centric design to withstand & recover from evolving threats”.

The results offer compelling empirical evidence in favor of H_o4. In the face of evolving cyber threats, an organization’s resilience and recovery capacity are greatly enhanced by a proactive cybersecurity strategy. Compared with organizations that rely solely on structural or resource-based advantages, those that integrate governance-driven strategy, flexibility, and integrated security controls are more resilient. These findings highlight the significance of switching from reactive security strategies to cybersecurity frameworks that are organized, proactive, and governance oriented. For more information on statistical data & Analysis, refer to Table 7.7 Appendix B.7: ANNOVA & Hierarchical M. Regression Analysis for RQ 4

Findings on RQ 5 & H_o5:

RQ 5: What policy frameworks and strategies based on industry best practices can be developed to enhance security while deploying emerging technologies in enterprises?

The fifth research question examines policy frameworks and strategies grounded in industry best practices to enhance security when deploying emerging technologies in enterprises. The fifth research hypothesis states:

"Implementing comprehensive security policies & frameworks and adhering to industry best practices significantly reduces the security risks associated with AI, IoT, and Blockchain integration".

The fifth hypothesis is cautiously and partially supported by the results. Although the link is complicated, cybersecurity event patterns are largely predicted by the quality of the policy framework. Organizations operating in high-risk or highly interconnected technology contexts may adopt stronger frameworks rather than merely reduce risk. These results highlight the need for strong leadership participation (H_o3) and the inclusion of proactive frameworks (H_o4) to effectively reduce cybersecurity risk, as policy implementation alone is insufficient. For more information on statistical data & Analysis, refer to Table 7.8 - Appendix B.8: ANNOVA for RQ 5 , Table 7.9 - Appendix B.9: Simple linear Regression for RQ 5.

Overall Model Findings:

Using multiple regression analysis, we examined the combined effects of emerging technology integration, cybersecurity leadership, and governance frameworks on organizational resilience. A multiple regression analysis test had organizational resilience as the dependent variable. Following independent variables were entered into the model which were integration level of emerging technologies, Leadership_Index, ET_Leadership interaction term, Proactive_Framework, and Policy_Framework_Strength. It was noted that all variables were entered simultaneously using the enter method.

For more details on Statistical data & analysis results, refer to Table 7.10 - Appendix B.10: Overall Model ANNOVA & Multiple Regression.

Test on Model Fit and Predictive Power

The overall regression model was statistically significant, with the result of the F test , $F(5,44) = 9.398$, $p < 0.001$. A value of 9.398 indicates that the model is finding significantly more patterns than noise. Generally, the higher this number, the more likely the results are meaningful, indicating that the set of predictors reliably explains variation in organizational resilience.

The model achieved an R^2 value of 0.516 and an adjusted R^2 of 0.461, demonstrating that approximately 51.6% of the variance in organizational resilience is explained by the combined governance, leadership, and framework-related variables. Given the modest sample size (n = 50), this represents strong explanatory power and confirms the robustness of the integrated model in explaining enterprise cybersecurity resilience.

The results made it very clear that resilience is not driven by a single factor but by the interaction among multiple organizational dimensions, particularly governance and framework strength.

Test on Effects of Emerging Technology Integration

The level of emerging technology integration did not emerge as a statistically significant predictor of organizational resilience in the final model ($\beta = -1.767$, $p = 0.348$). The findings here suggested that the intensity or dept of integration of emerging technologies does not independently determine an organization's ability to recover from or adapt to cyber threats when governance and framework variables are considered simultaneously.

This result reinforces earlier findings in the study, indicating that new technology adoption or integration of it alone is not inherently associated with either improved or weakened security

posture. Instead, resilience outcomes appear to depend on how these technologies are governed and secured rather than on their level of technical embeddedness.

Test on Effects of Leadership

The Leadership Index was not statistically significant in the presence of other predictors ($\beta = -2.426$, $p = 0.275$). This indicates that leadership does not exert a direct influence on organizational resilience once proactive and policy framework variables are included in the model. The interaction between leadership moderation of integration effects (ET_Leadership) was not statistically significant ($\beta = 3.248$, $p = 0.307$). Together, these results suggest that leadership does not directly enhance resilience nor it significantly moderated the relationship between technology integration and resilience within the full model. Instead the leadership effects appeared to operate indirectly, primarily through the establishment and strengthening of structured cybersecurity frameworks rather than through independent or moderating mechanisms.

Test on Effects of Proactive Cybersecurity Framework

The Proactive Framework variable representing the Proactive Framework model was identified as the strongest and most statistically significant predictor of organizational resilience ($\beta = 2.351$, $p < 0.001$). So, the organizations that report stronger proactive cybersecurity frameworks always demonstrated significantly higher resilience, reflected in improved capacity to recover from and adapt to cyber threats.

The statistical strength of the coefficient also indicated that governance-driven, strategically aligned, and future-focused cybersecurity frameworks are the central determinants of enterprise cybersecurity resilience. Among the variables included in the model, the proactive framework exerted the greatest influence on resilience outcomes, underscoring its critical role in enterprise cybersecurity governance.

Effects of Policy Framework Strength

Policy_Framework_Strength representing Policies, standards & procedures was also statistically significant ($\beta = -1.711$, $p < 0.001$). But the negative coefficient suggested that organizations with more formalized and stringent security policies reported lower perceived resilience. This pattern may reflect a much stricter internal evaluation, heightened compliance sensitivity, or the reactive strengthening of policies over the proactive, following previous security challenges rather than an absence of governance effectiveness.

Despite the negative direction, the statistical significance of this variable confirms that policy frameworks play an important role in shaping resilience perceptions, though their impact may be complex and context-dependent rather than uniformly protective in itself.

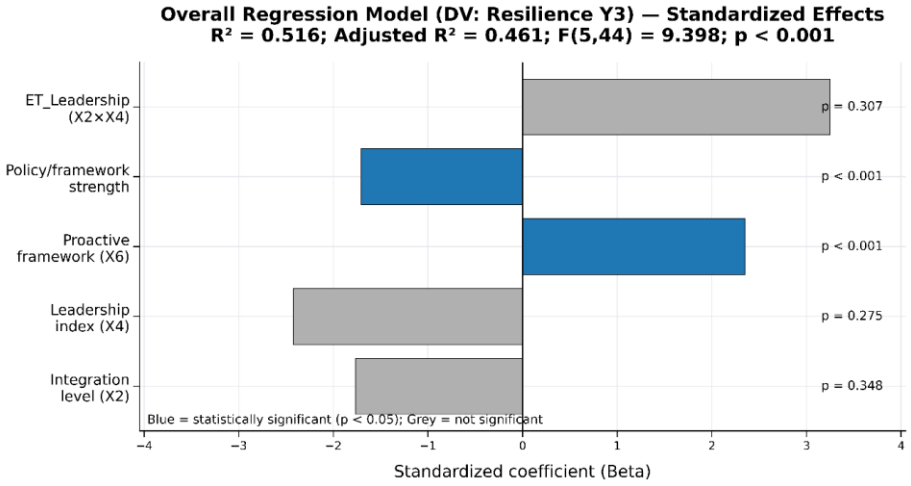


Figure 4.5

Standardized Effects (Beta) Plot - Overall regression Model

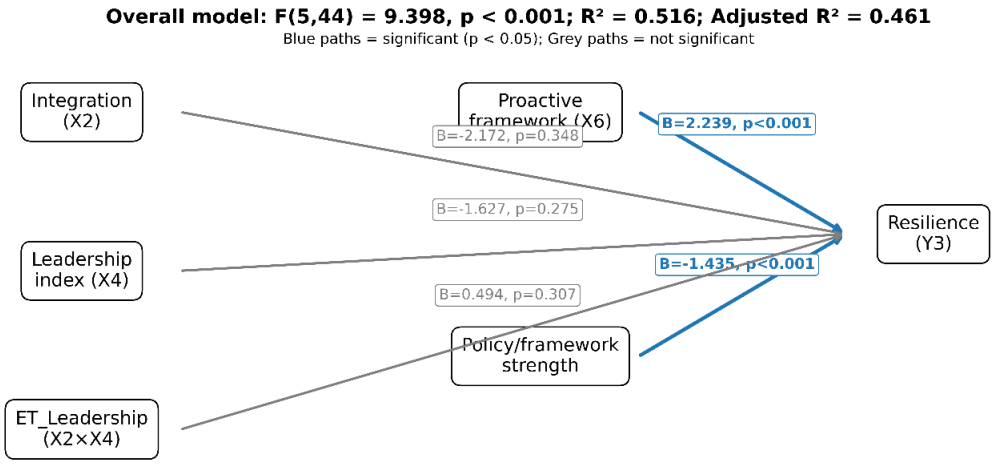


Figure 4.6

Overall Model - Significance of Variables

The above standardized effects (Beta) plot shows that the **Proactive Framework** has very significant influence on Output Variable , it has the strongest positive and statistically significant influence on organizational resilience, while **Policy/Framework Strength** also has a significant effect in the negative direction. While the **integration level**, **leadership index**, and the **ET_Leadership interaction** exhibited weaker standardized effects and were not statistically significant, consistent with the overall regression results. Refer to Table 7.10 - Appendix B.10: Overall Model ANNOVA & Multiple Regression for the detailed regression.

Overall Interpretation of the Integrated Model

The multiple regression model was statistically significant. The overall findings demonstrated that organizational resilience is primarily driven by the robustness of a proactive cybersecurity framework rather than by technology integration or leadership alone. Leadership and integration remain as important contextual factors; their influence on resilience appears to be mediated always through governance mechanisms and structured cybersecurity frameworks.

The strong explanatory power of the model, as indicated by the Coefficient of Determination ($R^2 = 0.516$), confirms that governance and framework-related variables collectively provide substantial insight into enterprise resilience against cyber threats.

Overall, the model indicates that technology adoption alone does not determine security posture. Enterprise resilience is primarily an outcome of planning, influenced by structured, proactive cybersecurity frameworks and governance mechanisms. Leadership contributes indirectly by fostering these frameworks rather than directly altering resilience outcomes. Further, it suggests that enterprises seeking to enhance resilience against evolving cyber threats should prioritize developing a robust framework and aligning governance over merely expanding technological integration.

4.5 Results from Case Study Analysis

For full details of each case study and their analysis, refer to Appendix A.5.

Case study Analysis Summary Table 4.12, shared below, presents the relationship between ET & other variables and the case study analysis results, including findings, results, & Conclusion.

Table 4.12

Case Study Analysis – Summary of Findings, Results, and Conclusions

Case Study / Source	Emerging Technology Focus	Key Variables Examined	Key Findings	Results	Conclusion (Short)
Yaacob, Idrus & Idris (2023)	AI, IoT, Blockchain	Integration Level (X2), Framework Robustness, Resilience (Y3)	Higher integration increases complexity and exposure when governance is weak; structured integration improves security maturity	Strong relationship between integration depth and framework robustness	Secure adoption depends on proactive, scalable cybersecurity frameworks rather than integration level alone
PricewaterhouseCoopers (2023)	Enterprise Digital Trust	Board Involvement, Cyber Readiness	Technology adoption outpaces cybersecurity readiness	Persistent governance gaps	Board-level governance is essential for cyber resilience
Kumar & Mallipeddi (2022)	Industry 4.0 (AI, IoT, Cloud)	Technology Integration, Cyber Risk, Operational Impact	Rapid digital transformation expands attack surface and operational risk	Increased cybersecurity risk without parallel framework maturity	Balanced integration with proactive governance mitigates risk and enhances resilience
Espíndola et al. (2022)	Emerging Technologies (Cross-sector)	Risk Management Adoption, Organizational Readiness	Successful ET adoption linked to internal capabilities and leadership support	Governance readiness determines risk management effectiveness	Organizational maturity and leadership enable secure ET adoption

Abrahams et al. (2024)	Cybersecurity Training (Human factor)	Training & Awareness (X5), Compliance, Culture	Awareness programs significantly improve employee security behaviour	Positive impact on compliance and incident response	Human factors are critical enablers of cybersecurity resilience
Adedamola Oluokun et al. (2024)	AI-driven Cybersecurity	Cybersecurity Investment, Leadership, Resilience (Y3)	Investment enables advanced detection and governance capabilities	Improved leadership effectiveness and cyber resilience	Strategic investment supports proactive frameworks and resilience
Akash Takyar (2023)	Regulatory Compliance	Policy Strength (X7), Assurance, Availability	Compliance improves baseline assurance but shows diminishing returns	Policies alone insufficient for resilience	Policies must be embedded within proactive governance frameworks
Li & Liu (2021)	Artificial Intelligence	AI Adoption, Incident Prevention	AI enhances threat detection but introduces new risks	Conditional reduction in incidents with proper controls	AI security benefits depend on governance and lifecycle controls
Okolo & Ighoroje (2024)	Banking Sector	Training, Compliance, Incident Response	Training and policy acknowledgement improve response times	Improved cybersecurity culture and responsiveness	Culture and training reinforce policy effectiveness
Hasan et al. (2022)	Blockchain (Smart Infrastructure)	Blockchain Integration, Security Challenges	Decentralization improves integrity but raises scalability risks	Mixed security outcomes	Blockchain security requires complementary governance and controls

Conclusion:

The reviewed case studies provide compelling evidence suggesting that investing in cybersecurity training and awareness programs, alongside securing top management support, is crucial for improving employee compliance with security protocols.

The case study analysis (Table) focused on outcome-focused conclusions, reinforcing the quantitative findings by demonstrating that emerging technology risks are primarily driven by framework robustness rather than technology adoption & integration level alone. Across multiple sectors and technologies, proactive cybersecurity frameworks and leadership-driven governance consistently emerged as the decisive factors influencing organizational resilience. It also collectively indicates a strong positive relationship between cybersecurity training and awareness programs and employee compliance with security protocols. These programs' effectiveness appears to stem from their ability to raise awareness, shape attitudes, and influence intentions toward compliance, ultimately resulting in improved protective behaviors. Such Trainings & awareness activities should be part of a proactive Cybersecurity framework which is continuously evolving which supports $H_0 4$ in this case as well.

So, Investment in a Proactive framework which if flexible & it covers a comprehensive cybersecurity training and awareness appears to be a worthwhile strategy for improving organizational security posture by fostering a culture of security compliance among employees.

4.6 Triangulation Findings & Results:

As illustrated in the Research Methods & Design section, Triangulation methodology below in ‘Figure 4.7 : Visual Triangulation – Outcome’s & Conclusion’ was followed to arrive at the consensus of this study, namely the Integrated findings from the case study analysis, the literature review outcome & the survey questionnaires' statistical analysis.

The figure below on ‘Visual Triangulation – Outcomes & Conclusion’, shows the results of each method used & the overall triangulated conclusion.

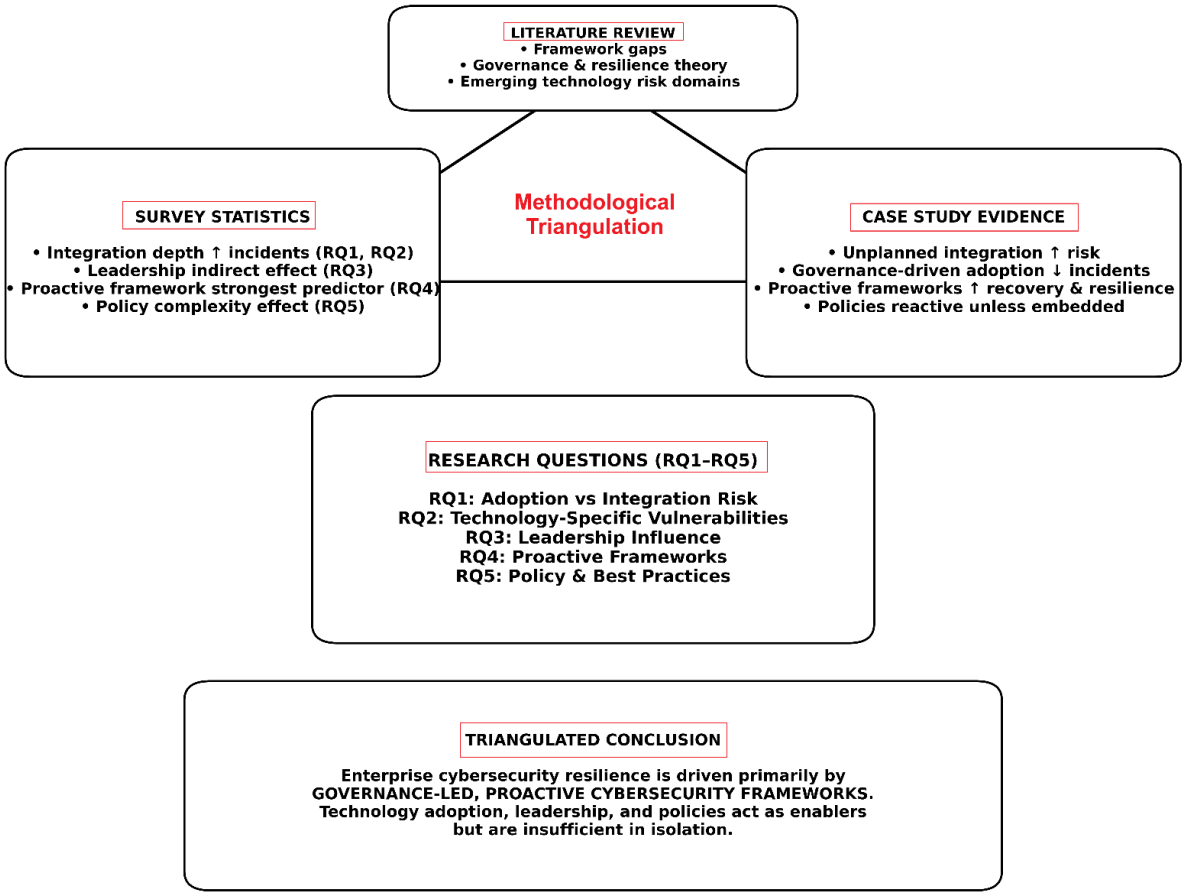


Figure 4.7

Visual Triangulation – Outcome's & Conclusion

According to the figure 'Visual Triangulation " & the 'Triangulation Summary' Table 4.13 , Triangulation results, Enterprise cybersecurity resilience in new technology settings primarily depends on proactive cybersecurity frameworks guided by governance, while leadership and policy are helpful but insufficient on their own.

Table 4.13

Integrated Triangulation Summary

Theme/Focus	Survey Statistics	Literature Review	Case Studies	Conclusion
ET Integration Risk	Significant	Strong support	Confirmed	Risk driven by depth, not adoption
Leadership	Indirect effect	Enabler role	Governance catalyst	Mediated influence
Proactive Framework	Strongest predictor	Strong consensus	Operationally validated	Primary resilience driver
Policy Strength	Complex/negative	Context-dependent	Reactive indicator	Insufficient alone

4.7 Summary of Research Questions Findings

This study examined the impact of emerging technologies—Artificial Intelligence (AI), the Internet of Things (IoT), and Blockchain on the enterprise information security. The findings showcased that the adoption of emerging technologies increased the complexity of enterprise security management, the higher levels of technology integration significantly showcased increased risks & cybersecurity incidents due to expanded attack surfaces and system complexity, while structured and formally governed adoption reduced the risk (RQ1). The integration of emerging technologies was found to significantly correlate with vulnerability-driven cybersecurity exposures, particularly related to privacy issues, governance gaps, and implementation weaknesses, confirming that such unplanned integration amplified specific vulnerability domains when security controls did not evolve alongside technology (RQ2). The results of analysis further indicated that information security leadership positively influenced secure adoption and implementation outcomes; however, there was a reduction in cybersecurity incidents with active senior leadership involvement rather than just a leadership commitment or policy presence alone (RQ3). Proactive, governance-driven cybersecurity frameworks were found to be significantly enhancing organizational resilience and recovery capability, providing strong empirical support for the effectiveness of proactive frameworks over reactive or compliance-driven approaches (RQ4). Finally, while the strength of the security

policy framework was significantly associated with cybersecurity incident patterns, the relationship was complex, indicating that policies alone are insufficient to reduce risk unless reinforced by leadership engagement and proactive governance (RQ5). Further, the triangulation results confirm that policies alone are insufficient and must be operationalized through proactive frameworks and leadership engagement, thereby supporting H_o5.

CHAPTER 5

DISCUSSION, IMPLICATIONS, RECOMMENDATIONS AND CONCLUSIONS

5.1 Introduction

This study addressed the growing information security challenges posed by the integration of emerging technologies, such as artificial intelligence, the Internet of Things, and blockchain, into enterprise IT environments. The research problem focused on how growing technological complexity, expanded attack surfaces, and governance gaps affect cybersecurity incidents, vulnerabilities, secure implementation, and organizational resilience.

The Main purpose of the study was to empirically examine the relationships between emerging technology adoption and integration, cybersecurity outcomes, leadership involvement, and the effectiveness of proactive cybersecurity frameworks. A quantitative research approach was employed using a structured survey Questionnaire using likert scale format which was administered to professionals with experience in IT and cybersecurity. As part of Statistical analysis, Regression and hierarchical regression analyses were performed to test the Null hypotheses listed in this study.

All Ethical considerations were addressed through informed consent , voluntary participation, and the protection of respondents' anonymity and confidentiality, with all data used solely for academic purposes.

This chapter would translate the empirical findings presented in Chapter 4 (Results) into a much practical recommendations. Each recommendation is explicitly grounded in the statistical results and aligned with the study's hypotheses. Those recommendations focused on technology governance & its integration, structured adoption, vulnerability management, leadership engagement, proactive cybersecurity frameworks, policy review, and training and awareness initiatives.

5.2 Discussion on Hypothesis Testing Results

5.2.1 H_o1 Results

Hypothesis(H_o1): The adoption of AI, IoT, and blockchain technologies increases the complexity of enterprise security management, leading to cybersecurity breaches & incidents.

The first research hypothesis was partially supported, indicating that a higher level of technology integration is associated with cybersecurity vulnerabilities. However, when these technologies

are integrated into a well-designed governance plan, structured technology adoption appears to reduce risk, even as the level of integration increases incidents.

On similar lines, Bako et al. (2025) suggested that the combination of blockchain technology and artificial intelligence offers a fresh approach to cybersecurity tactics. All of them, however, require some thought, including laws and regulations, technological issues, and a shortage of skilled labor. General suggestions for increasing adoption include educational initiatives to develop sufficient workforce competencies in these convergent technologies, cross-organizational collaboration models, and sectoral best practices to be followed when putting the concepts and frameworks discussed into practice. Salama et al. (2024) suggested that cybersecurity requires the use of AI. AI is necessary for cybersecurity defense against attacks and blockchains as they are known to provide good detection capabilities. Blockchain is the key technology behind the popular cryptocurrency Bitcoin. A blockchain is an open ledger not controlled by any single entity and accessible to all users. It is a technology that facilitates honest and transparent communication between people and businesses. Beyond its benefits, digital currency is becoming more popular and changing how companies operate.

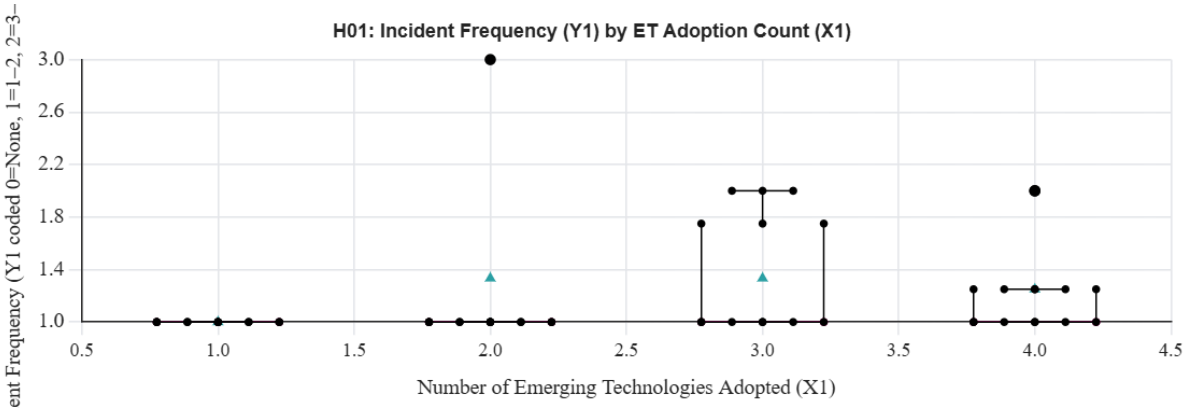


Figure 5.1

$H_0 1$ — Incident Frequency (Y1) by ET Adoption Count (X1)

In the above box plot, the visual pattern is consistent with the statistical results, where the regression analysis shows a significant relationship between ET adoption and incident frequency, even though the differences are not strongly separated in the box plot.

5.2.2 $H_0 2$ Results

Hypothesis (H_o2): Integrating emerging technology into enterprise systems significantly correlates with increased specific vulnerabilities, such as data privacy issues and scalability concerns.

The findings for the second research hypothesis indicated that the integration of emerging technologies is linked to vulnerability-driven cybersecurity exposures. When incorporating new technologies into corporate systems, the findings emphasize the significance of adaptive cybersecurity frameworks, secure-by-design principles, and proactive risk assessment. On the contrary, Goundar and Gondal (2025) reported a notable increase in detection precision, with accuracy rising from 85.2% to 93.4% . The blockchain layer ensured that AI judgments and alarms were tamper-proof and verifiably recorded. For applications where security and traceability are crucial, the trade-off between increased delay and decreased throughput proved acceptable. Saleh et al. (2024) demonstrated the great potential for combining decentralized AI algorithms with blockchain technology. By enabling safer and more effective information exchange, threat identification, and response, it has the potential to completely transform cybersecurity. However, several challenges and limitations, including scalability, interoperability, and regulatory concerns, must be overcome to accomplish this successfully. Blockchain-based cybersecurity platforms and decentralized AI systems are examples of current technologies that have demonstrated potential in resolving these problems. However, there is still room for improvement and further research to provide more dependable solutions.

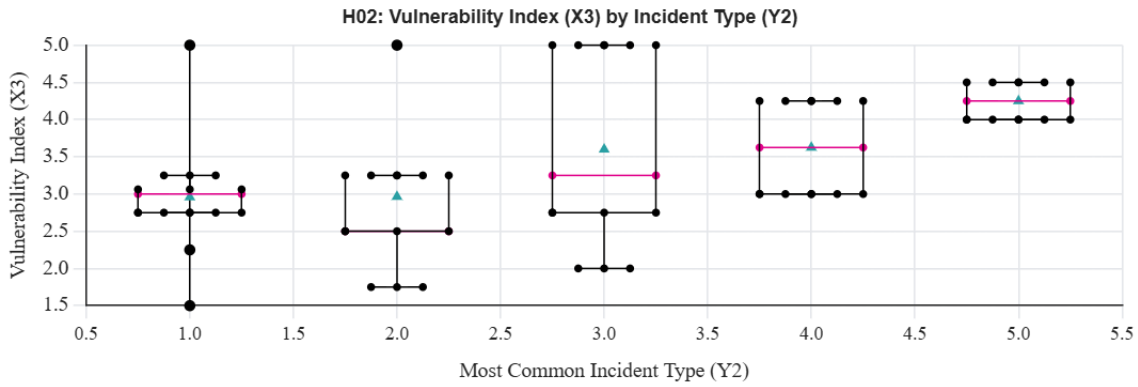


Figure 5.2

H_o2 Vulnerability Index (X3) by Incident Type (Y2)

The box plot above reveals notable differences in vulnerability index distributions across different types of incidents. Incidents like **Data theft and ransomware incidents** were associated with higher median vulnerability scores and wider dispersion, indicating greater underlying exposure factor and structural weaknesses. In contrast, incident categories such as service disruption show relatively lower median vulnerability and narrower interquartile ranges. These distributional differences overall suggests that organizations experiencing more severe incident types tend to exhibit higher levels of technological vulnerability, providing the required visual support for H_o2.

5.2.3 H_o3 Results

Hypothesis (H_o3): Strong information security leadership positively influences the secure adoption and implementation of Emerging technologies, reducing the likelihood of security breaches.

The third research hypothesis was partially supported by empirical evidence. The findings indicated that leadership commitment significantly enhances secure adoption and implementation of emerging technologies. This underscores the importance of active leadership involvement in cybersecurity decision-making to reduce security breaches. Where leadership is accountable, cybersecurity is more robust. Aniebonam et al. (2025) highlight how crucial transformative leadership is to advancing cybersecurity innovation. For their companies to remain competitive amid evolving cyber threats, visionary leaders are essential for coordinating technology advancement with security requirements. Transformational leaders may ensure their companies are secure and technologically advanced by fostering an innovative culture and keeping an eye on the future. Businesses should fund leadership development initiatives that emphasize the value of cybersecurity knowledge and forward thinking. Sultana et al. (2024) affirm that AI greatly improves organizational resilience and data protection. Strong AI plans, supporting legislation, and integrated data methods all have a significant impact on its performance. Businesses should make investments in advanced data protection, AI-enhanced security solutions, and compliance with national cybersecurity laws. To optimize advantages, leadership dedication, moral AI governance, and thorough staff training are essential. To preserve security performance and guarantee fair AI deployment across all organizations, cross-sector cooperation and ongoing innovation are advised.

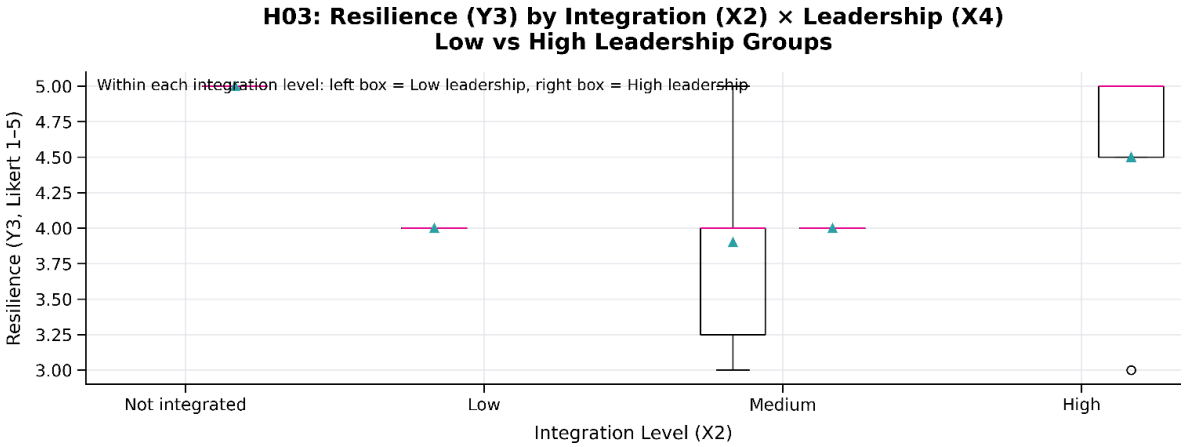


Figure 5.3

$H_0$3 Resilience (Y3) by Integration (X2) × Leadership (X4)

The box plot shows that organizations with a better leadership program and higher leadership involvement consistently exhibited higher resilience across all levels of technology integration, with the separation between low and high leadership groups increasing at the medium and high integration levels. This aligns with the significant positive interaction effect (X2 × X4) reported in the moderation regression results (see Table 34), indicating that leadership strengthens the relationship between integration and resilience. In Summary, the distribution supports $H_0$3 by visually reinforcing the moderating influence of leadership on the integration–resilience relationship.

5.2.4 $H_0$4 Results

Hypothesis ($H_0$4): A proactive cybersecurity framework may combine risk-driven strategy, strong culture and governance, and advanced technical controls with resilience and user-centric design to withstand & recover from evolving threats.

The outcome of testing the fourth research hypothesis indicates that an active cybersecurity framework significantly enhances the organization's resilience and recovery capability in the face of evolving cyber threats. The findings indicated the importance of adopting proactive cybersecurity approaches and structured, governance-oriented frameworks. Kanaan et al. (2024) provide a thorough model of cyber resilience to help companies defend against, mitigate, and recover from cyberattacks. With a focus on scalability, flexibility, and integration with existing

systems, the model highlights the importance of corporate culture and leadership in promoting cyber resilience. The advantages of the concept are acknowledged, but there are drawbacks as well, including organizational attitude, resource limitations, and the ever-changing nature of cyber threats. Safitra et al. (2023) showed that companies may improve their cybersecurity resilience in a variety of ways. These actions include creating tried-and-true incident response plans, implementing appropriate preventive measures, being more flexible in addressing new threats, and working with other parties to strengthen cybersecurity resilience. Organizations may protect themselves from cyberattacks and carry on with their business as usual by implementing these precautions. In order to achieve cyber resilience, the study highlights the significance of organizational leadership, responsibility, and innovation.

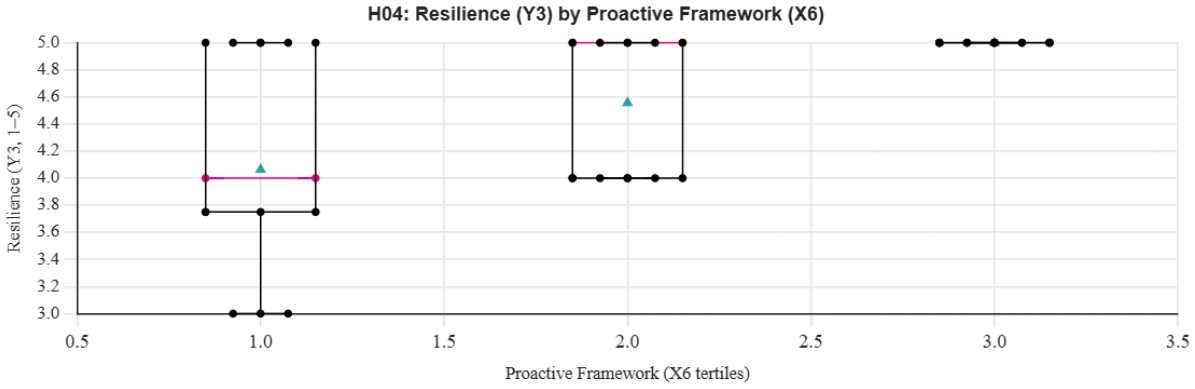


Figure 5.4

H_o4 Resilience (Y3) by Proactive Framework (X6)

The box plot showed that any organizations in the low proactive framework group displayed lower median resilience and greater variability, suggesting uneven preparedness and lower adaptive capacity. Overall, the distributional pattern supports H_o4 by visually indicating a positive association between proactive cybersecurity frameworks and organizational resilience.

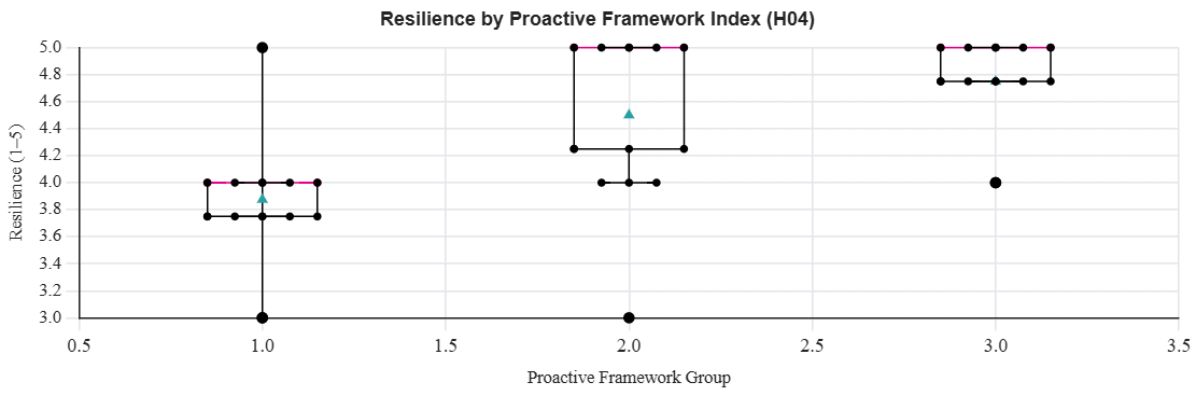


Figure 5.5

Resilience by Proactive Framework - H_o4 (X6 → Y3)

The box plot on Proactive Framework reinforces that organizations scoring higher on proactive framework measures—such as adaptability, interoperability in case of different scenarios, and the need for enhanced security strategies—demonstrate systematically stronger resilience outcomes. The progressive increase in medians from low to high framework groups indicates that proactive governance and forward-looking security principles & design are closely associated with improved recovery and adaptation capabilities. The pattern is consistent with the hypothesized direction in H_o4 , hence it complements the regression results reported earlier.

As per the Box plot with better Proactive Framework resilience always improved & was the best with completely proactive & pre-emptive framework.

5.2.5 H_o5 Results

Hypothesis (H_o5): Implementing comprehensive security policies & frameworks and adhering to industry best practices significantly reduces the security risks associated with AI, IoT, and Blockchain integration.

The fifth research hypothesis was partially supported, indicating that although the relationship is complicated, cybersecurity event patterns are largely predicted by the quality of the policy framework. Hence, organizations, especially those vulnerable to cybersecurity attacks, should implement robust policies to address them. Lubua and Pretorius (2019) proposed a framework for cyber policy that includes seven main themes: Data security, the control of the Internet and network services, the usage of company-owned devices, physical security, incident reporting and management, monitoring and compliance, and administrative concerns related to policies. The report suggests using this framework to make sure the cybersecurity policy is thorough. Lack of

information on policy-creation processes, inability to engage key stakeholders, lack of established rules, and lack of policy review are among the factors contributing to the absence of a complete policy. The organization's cybersecurity policy or other rules must serve as the basis for all of these actions. Hossain et al. (2024) suggested a policy framework that has several elements in common with the Cybersecurity Framework (CSF) of the National Institute of Standards and Technology (NIST). However, our policy framework guides local governments (LGs) in creating effective cybersecurity policies without overlooking important aspects, while the NIST CSF serves as an evaluation tool for any organization's cybersecurity posture. Our cybersecurity policy framework's genuine originality and value lie in its customized approach to addressing specific issues in LG operations, even though most of the sub-items under its seven main components are generally applicable to other organizational contexts.

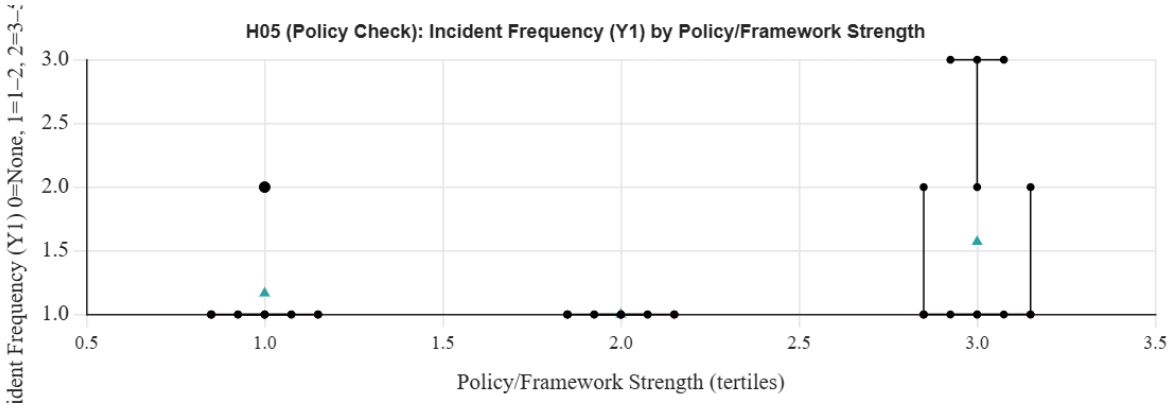


Figure 5.6

H_o5- Incident Frequency (Y1) by Policy/Framework Strength

The box plot shows largely overlapping distributions of incident frequency across low, medium, and high policy/framework groups, with no clear or consistent separation in median values. This visual pattern is consistent with the H_o5 statistical testing results, which indicate that policy and framework strength do not have a statistically significant direct effect on incident frequency, and therefore H_o5 was not supported for the incident outcome.

5.2.6 Summary of Hypothesis Results

Table 5.1

Hypothesis Support Matrix

Hypothesis	Supported ☑	Partially ☑	Not Supported ✗
H_o1		✔	
H_o2	✔		
H_o3		✔	
H_o4	✔✔		
H_o5			✔

✔✔ - Indicates very Strong.

Table 5.2

Hypothesis Results & Summary Table

Hypothesis	Variable Relationship	Statistical Test Applied	Key Result	Status
H_o1: The adoption of AI, IoT, and Blockchain technologies increases the complexity of enterprise security management, leading to cybersecurity incidents.	IV: Emerging Technology Adoption & Integration → DV: Cybersecurity Incidents	Multiple Regression (ANOVA & Coefficients)	Integration level positively associated with incidents ($\beta = 0.391$, $p = 0.007$); structured adoption negatively associated with incidents ($\beta = -0.571$, $p < 0.001$)	**Partially Supported**
H_o2: Integrating emerging technologies significantly correlates with increased enterprise vulnerabilities.	IV: Vulnerability Exposure → DV: Type of Cybersecurity Incident	Linear Regression (ANOVA)	Vulnerability significantly predicts incident type ($F = 6.839$, $p = 0.012$)	**Supported**

H_o3: Strong information security leadership positively influences secure adoption and implementation of emerging technologies.	IV: Leadership Commitment & Involvement → DV: Secure Implementation / Incidents	Hierarchical Regression	Leadership improves secure implementation; active leadership involvement associated with reduced incidents	**Partially Supported**
H_o4: A proactive cybersecurity framework enhances organizational resilience.	IV: Proactive Framework Index → DV: Organizational Resilience	Regression Analysis	Proactive framework strongly predicts resilience ($\beta = 0.643$, $p < 0.001$)	**Strongly Supported**
H_o5: Comprehensive security policies and frameworks reduce cybersecurity risks associated with emerging technologies.	IV: Policy Framework Strength → DV: Cybersecurity Incidents	Multiple Regression	Policy strength significantly associated with incident patterns ($\beta = 0.448$, $p = 0.012$); effect context-dependent	**Partially Supported**

5.3 Discussion on Triangulation Results

Table 5.3

Triangulation Matrix: Survey × Literature Review × Case Study × Research Questions

Research Question	Survey Statistics (Quantitative Evidence)	Literature Review (Theoretical & Empirical Support)	Case Study Evidence (Practical Validation)	Triangulated Interpretation
RQ1: Security implications of emerging technology adoption	Regression analysis showed that *integration depth* significantly increased cybersecurity incidents, while adoption alone did not	Literature consistently reports increased complexity, attack surfaces, and decision-making challenges arising from rapid ET adoption	Case studies demonstrated higher incidents in organizations with unplanned or accelerated integration	Security implications stem from **unmanaged integration**, not from adoption itself

RQ2: Vulnerabilities and risks associated with integration	Vulnerability index significantly correlated with incident types and exposure patterns	Studies identify AI lifecycle risks, IoT endpoint insecurity, and blockchain smart-contract flaws as integration-driven	Case studies confirmed technology-specific vulnerabilities emerging post-integration	Integration amplifies **technology-specific vulnerabilities** unless mitigated proactively
RQ3: Influence of cybersecurity leadership	Leadership index not a direct predictor of resilience but showed indirect influence through frameworks	Leadership literature emphasizes governance, culture, and accountability as mediators of security outcomes	Case studies showed executive sponsorship enabled framework institutionalization	Leadership acts as an **enabling and moderating factor**, not a standalone control
RQ4: Framework deficiencies and proactive framework requirements	The proactive framework variable was the **strongest predictor of resilience** in the overall model	Literature criticizes static, compliance-driven frameworks and supports adaptive, hybrid models	Case studies demonstrated faster recovery and adaptability with proactive frameworks	**Proactive, governance-driven frameworks** are the primary drivers of resilience
RQ5: Role of policies and best-practice frameworks	Policy framework strength significant but with a negative coefficient, indicating complexity	Literature explains policy-heavy environments often reflect reactive governance	Case studies showed policies strengthened post-incident with limited resilience gains	Policies are **necessary but insufficient** without proactive governance and execution

As per the Triangulation matrix Table, which showcased the connection of RQ's with LR, Surveys & Case Study

RQ1 (Security implications of adoption): Demonstrates that risk emerges from unmanaged integration, not adoption itself.

RQ2 (Vulnerabilities & risks): Confirms technology-specific vulnerabilities amplified by integration depth.

RQ3 (Leadership influence): Shows leadership's indirect, enabling role via governance and culture.

RQ4 (Framework deficiencies & proactive design): Validates proactive, hybrid frameworks as central to resilience.

RQ5 (Policy & best practices): Explains why policies must be embedded within proactive frameworks.

The case study analysis summarized in the table above complements the quantitative findings by providing practical and contextual validation of the research results. Across all cases, cybersecurity risk was found to be driven primarily by framework robustness followed by governance maturity and integration depth, rather than technology adoption alone. Leadership and policy mechanisms consistently emerged as enabling factors, with their effectiveness dependent on their integration into **proactive cybersecurity frameworks.**

5.4 Implications

This study has important implications for theory, research, and enterprise practice in relation to emerging technology adoption and enterprise information security. The implications are derived directly from the empirical findings and are aligned with the research questions (RQ1–RQ5) and the conceptual framework developed in this study.

5.5 Theoretical Implications

The findings reinforce the view that emerging technologies should be understood as **socio-technical systems**, rather than isolated technical artifacts. The results demonstrate that **technology integration depth**, rather than adoption alone, is a key determinant of cybersecurity risk. This refines traditional risk and security theories by highlighting the limitations of static frameworks when applied to highly integrated environments involving AI, IoT, and Blockchain (RQ1, RQ2).

The strong relationship between proactive cybersecurity frameworks and organizational resilience provides empirical support for **cyber resilience theory**, confirming that governance-driven, adaptive security approaches are more effective than reactive or compliance-only models (RQ4). This supports a theoretical shift from control-centric security toward resilience-oriented frameworks.

The study also contributes to cybersecurity leadership theory by empirically validating leadership as a **moderating factor** in secure technology adoption. While leadership commitment improves secure implementation, the reduction of cybersecurity incidents is significantly associated with **active senior leadership involvement** rather than the presence of policies or formal roles alone (RQ3). This reinforces the importance of leadership behavior and engagement in shaping cybersecurity outcomes.

Finally, the partial support for policy-focused hypotheses suggests that policy and compliance theories require contextual refinement. The findings indicate that security policies function as **enablers rather than guarantees** of risk reduction and are effective only when combined with proactive governance and leadership engagement (RQ5).

Implications by Research Question

RQ1 – Security Implications of Emerging Technology Adoption:

The positive relationship between integration level and cybersecurity incidents implies that emerging technologies increase security risk primarily through system complexity , expanded attack surfaces due to vulnerabilities & newer attack landscape & Attack vectors Strategic decision-making is the key here , enterprises must therefore treat integration depth as a critical risk variable rather than a purely operational or innovation-driven choice.

RQ2 – Vulnerabilities and Risks of Integration:

There was a significant association between vulnerability exposure and incident types, indicating that emerging technology integration amplified risks in the specific vulnerability domains, including privacy, scalability, and governance gaps. This implies that the enterprise vulnerability management component of Enterprise Risk Management (ERM) must be embedded throughout the technology integration lifecycle rather than applied as a post-deployment activity.

RQ3 – Role of Cybersecurity Leadership:

The findings showed that cybersecurity leadership influences outcomes through engagement rather than structure. This implies that enterprises should position cybersecurity leadership as a strategic governance function, with direct executive participation in decision-making and oversight, rather than making it as a delegated technical responsibility.

RQ4 – Proactive Cybersecurity Frameworks:

The strong predictive relationship between proactive frameworks and resilience implies that enterprises should move away from reactive approaches or compliance-driven approaches. Todays world needs Hybrid, adaptive frameworks that integrate leadership,governance and risk-driven strategy to manage emerging technology risks.

RQ5 – Policy Frameworks and Best Practices:

The partial support for policy-centric hypotheses suggests that strong policies alone do not ensure risk reduction or can address the issues. Policies must be continuously reviewed for alignment with all aspect of businesses, it should be reinforced through leadership involvement and proactive governance to remain effective in dynamic, technology-intensive environments. Overall Implications Collectively, the findings indicate that enterprise information security in the context of emerging technologies is shaped by the interaction between technology integration, leadership engagement, governance frameworks, and organizational culture. Effective cybersecurity outcomes depend not on isolated controls or policies, but on a well-connected, holistic, governance-driven approach that embeds security into technology adoption and the organizational decision-making process. Practices like security by design and security by default should be embedded in the process of developing systems.

Overall, the implications discussed above highlight that emerging technology risks cannot be effectively addressed by isolated technical, administrative, or policy or framework controls. Instead, the findings emphasize the need for governance-driven strategies, active leadership engagement, proactive hybrid, integrated cybersecurity frameworks, continuous organizational adaptation, & Continous monitoing & improvement of systems through feedback & leasson learnt. Working on implications, we would move to recommendations that translate the empirical findings into actionable guidance for enterprises seeking to adopt emerging technologies while strengthening their information security posture. Finally, to conclude, the mixed results associated with policy framework strength indicate that policies should not be viewed as standalone risk controls. Instead, they should be continuously reviewed and reinforced through proactive governance and leadership engagement. As we know a Policy alone with a pro, a Policy alone with proper enforcement & practice doesn’t bring much benefitper enforcement & practice doesn’t bring much benfit at all .

5.6 Recommendations

Based on the empirical results of the Analysis & Study, the following recommendations are derived directly from the statistical test-based findings:

1. ET Integration Governance: Organizations should treat the level of emerging technology integration as a measurable risk factor, as higher integration levels are associated with increased cybersecurity incidents. Governance measures should be in place before any new technology is adopted.
2. Structured Technology Adoption: Formal and governed adoption processes should be implemented to reduce risks linked to informal or fragmented technology integration.
3. Vulnerability Management: A more structured vulnerability assessment is required in case of ET adoption, it should be applied before any such adoption, it should focus on privacy exposure, governance gaps, and implementation weaknesses & risks identified during integration.
4. Leadership Engagement: Senior leadership should be directly involved in cybersecurity decision-making. While leadership commitment supports secure implementation, active involvement is essential for reducing incident frequency.
5. Proactive Cybersecurity Frameworks: Organizations should prioritize proactive measures and develop or use Hybrid Governance-driven cybersecurity frameworks that emphasize adaptability to support newer technology. Integration, scalability, interoperability, and risk-driven strategy to enhance resilience.
6. Policy Framework Review: Security policies and frameworks should be evaluated in a timely manner in the context of organizational change, exposure to newer technology adoption, and incident history, recognizing that policy strength alone may not guarantee risk reduction. Continuous improvement should be the focus of the review & update, it should be done in the context of organizational exposure and supported by proactive governance structures.
7. Training and Awareness: Regular cybersecurity training programs should be sustained and aligned with emerging technology risks to maintain employee compliance and incident responsiveness.

These recommendations are fully aligned with empirical results which is the result of statistical analysis & the Triangulation between the Literature review , case study Analysis & Surveys and are derived directly from the statistical analysis presented in this study. So, a Proactive

Cybersecurity Framework would help organizations to tackle majority of the problems arising due to newer technology integration.

5.6.1 Recommendations for Practical Applications

Based on the empirical results observed, practical recommendations should prioritise governance actions that are directly supported by the study's findings. First, organizations should manage the integration intensity of emerging technologies as a defined risk factor. The results indicate that technology integration level is associated with incident frequency in the incident model, and that structured adoption practices can mitigate incident outcomes. Therefore, enterprises should not treat integration as a purely technical deployment decision but as a governance and risk decision that requires oversight and monitoring aligned with integration depth.

Second, organizations should formalize structured adoption and implementation controls for emerging technologies. The findings show that "adoption" behaves differently from "integration," supporting the need for formal adoption planning and implementation discipline rather than informal or fragmented deployment. This includes setting clear Goals, ownership, defining implementation stages, and ensuring security controls are embedded during implementation rather than retrofitted after integration, principle of security by Design & by default to be followed.

Third, enterprises should strengthen vulnerability management for emerging technologies by focusing on the vulnerability dimensions captured in the study (privacy exposure, governance gaps, implementation weaknesses). The significant association between the Vulnerability Index and incident patterns supports the practical need for structured vulnerability assessment in environments integrating AI, IoT, and Blockchain. Organizations should embed vulnerability review checkpoints during the adoption at the test phase and integration phases to reduce exposure that influences incident outcomes.

Fourth, organizations should treat cybersecurity leadership as an operational resilience enabler. The results show leadership is a significant predictor of resilience in the resilience model, but leadership does not significantly moderate the integration–resilience relationship. Practically, this supports strengthening leadership engagement through governance routines that build resilience capacity (rather than relying on leadership to offset integration risk through

moderation).

Fifth, organizations should prioritize building and maintaining a proactive cybersecurity framework, as a strong proactive framework is a significant predictor of resilience and improves the explanatory power of the resilience model when included. This supports a practical emphasis on strengthening proactive governance and robust frameworks as central mechanisms for improving resilience and recovery capability.

Finally, where policy frameworks are used, they should be treated as part of a broader governance mechanism rather than a standard-reduction tool. The $H_0 5$ results indicate integration does not significantly predict incident frequency and mediation was not processed under the stated conditions. In practice, this implies that policy and governance mechanisms may be better positioned to influence the broader security posture and resilience, rather than directly lowering reported incident counts in this dataset. This study examined the impact of emerging technologies—Artificial Intelligence (AI), the Internet of Things (IoT), and Blockchain on enterprise information security. The findings showcased that the adoption of emerging technologies increased the complexity of enterprise security management, the higher levels of technology integration significantly showcased increased risks & cybersecurity incidents due to expanded attack surfaces and system complexity, while structured and formally governed adoption reduced the risks (RQ1). The integration of emerging technologies was found to significantly correlate with vulnerability-driven cybersecurity exposures, particularly related to privacy issues, governance gaps, and implementation weaknesses, confirming that such unplanned integration amplified specific vulnerability domains when security controls did not evolve alongside technology (RQ2). The analysis further indicated that information security leadership positively influenced secure adoption and implementation outcomes; however, there was a reduction in cybersecurity incidents with active senior leadership involvement, rather than just leadership commitment or policy presence alone (RQ3). Proactive, governance-driven cybersecurity frameworks were found to significantly enhance organizational resilience and recovery capability, providing strong empirical support for the effectiveness of proactive frameworks over reactive or compliance-driven approaches (RQ4). Finally, while security policy framework strength was significantly associated with cybersecurity incident patterns, the relationship was complex, indicating that policies alone are insufficient to reduce risk unless reinforced through leadership engagement and proactive governance (RQ5).

Recommendations for Future Research

Future research should address methodological and measurement areas highlighted by the present findings. **First,** replication with a larger sample size is recommended to strengthen statistical power and generalizability, especially where relationships were weak or non-significant (e.g., the direct effect of integration on incident frequency in the H_o5 incident model).

Second, future studies should improve measurement precision for incident outcomes. In this study, "most common type of incident" included a large "Other" category, and the incident type variable's coding influences the coefficient direction in the H_o2 model. Future research should use a more granular incident taxonomy and ensure consistent coding to enable clearer interpretation of directionality and effect meaning.

Third, future research should extend validation of composite indices used in the study (e.g., Vulnerability Index, Leadership Index, Proactive Framework). While the study references acceptable internal consistency thresholds, future work should report full reliability outputs and, where possible, confirm construct validity through additional validation steps, thereby strengthening the robustness of index-based modelling.

Fourth, because leadership effects were significant for resilience, but moderation effects were not significant, future research should examine alternative modelling approaches to better test indirect pathways (for example, whether leadership influences resilience primarily through framework strength, as suggested by changes in significance when proactive framework variables are introduced).

Finally, future studies should examine outcomes beyond incident frequency, given the study's results that certain governance variables may influence broader security posture and resilience rather than incident counts directly. Expanding the dependent variables to include resilience-related measures (as used here) and governance maturity measures would enable a more comprehensive evaluation of how policies and frameworks affect enterprise information security in emerging technology contexts.

Unified Integrated Frameworks

A unified framework becomes critical as enterprises move toward continuous digital transformation; security challenges will be dynamic, adaptive, and cross-domain, requiring

governance-led, proactive, and resilience-focused frameworks that can evolve alongside technology rather than react after incidents occur.

For more details of Unified Integrated Frameworks for AI , IoT, kindly refer to Appendix D .

D.1 Unified AI Framework

D.2 Unified IoT Framework

D.3 General Blockchain Assessment Framework

Unified Framework – Critical Controls for IOT

The unified framework combines the core functions of the NIST CSF, IR 8259, SP 800-53, CSA IoT, OWASP IoT Top 10, IoTSF, MITRE, CMMC, and ISMS 27001 to create a unified, consolidated, simplified framework & control guide for enterprises.

More details: Refer to **Appendix D.2** Table 7.18 for Unified Framework - Controls Implementation & Critical Controls List.

General Framework for Blockchain

Blockchain offers a greater level of transparency & integrity due to its nature & architecture of being shared & distributed allowing anyone with permission to access the entire transaction history with necessary permission, as we have understood that not all blockchain implementations are same, according to Spencer-Hicken, Schutte and Vlok (2023), " two categories permissioned & permissionless creates four blockchain types to be identified: public permissionless, private permissionless, private permissioned, private permissionless, further it was noted that Private permissionless blockchains had no use case currently because of contradicting properties" (Spencer-Hicken et al., 2023).

Therefore, I recommend a general hybrid framework applicable to all types. For more details, refer to **Appendix D.3**

5.6.2 Recommendations - Unified Proactive Cybersecurity Framework for Secure Adoption of ET's

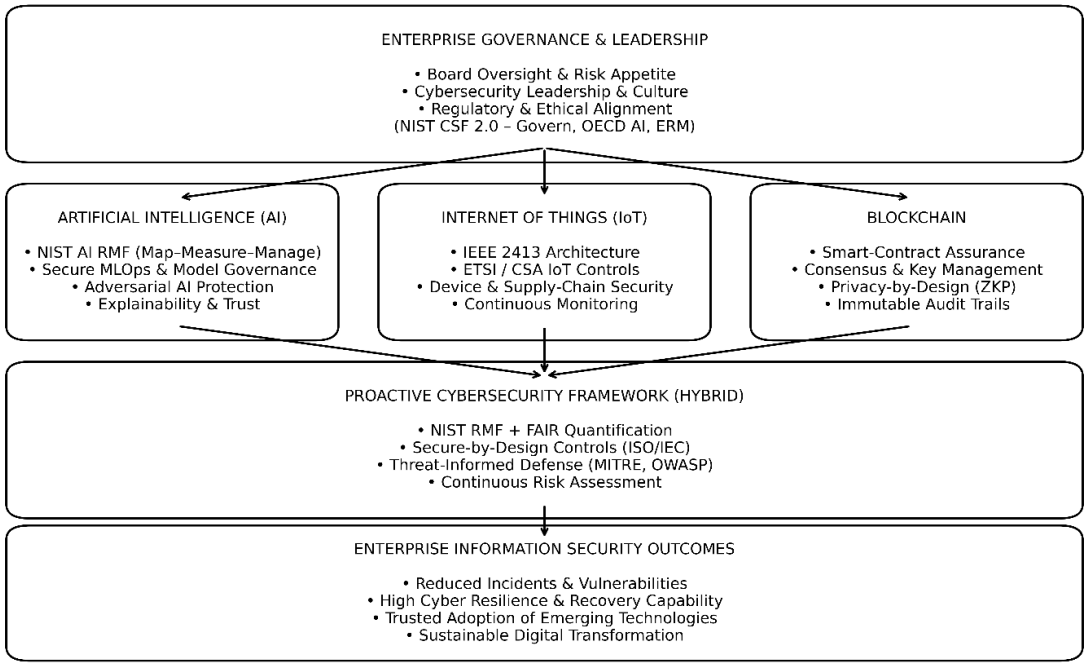


Figure 5.7

Unified Meta-Framework for Secure Adoption of Emerging Technologies

Above Unified Meta Framework provides the single holistic unified view of frameworks that can be used for adoption of ET's, clearly shows governance → framework → outcomes flow. It also supports the key statistical findings that Proactive framework = strongest predictor of resilience, also aligns itself with Aligns cleanly with RQ4 & RQ5 and your policy recommendations.

The findings of the statistical analysis & the study clearly demonstrate that enterprise cybersecurity resilience in environments adopting emerging technologies is not determined by technology adoption or integration alone, but by the presence of a structured, proactive, and governance-driven cybersecurity framework. Based on empirical results and supported by integrated theoretical and conceptual foundations, this section proposes a Unified Meta-Framework to guide enterprises in the secure adoption of technologies such as Artificial Intelligence (AI), the Internet of Things (IoT), and Blockchain.

This proposed framework addresses the deficiencies identified in existing single-framework

approaches and addresses the study's core research questions, particularly RQ4 and RQ5. It integrates governance, leadership, risk management, technical controls, and resilience principles into a cohesive model adaptable across the emerging technology domains.

Governance and Leadership as the Foundational Layer, but at the apex of the unified framework is enterprise governance and cybersecurity leadership. This study identified Governance as a critical enabler of secure technology adoption. Although leadership did not emerge as a direct predictor of resilience in the overall regression model, its influence was found to be indirect, mediated by the establishment of structured and proactive cybersecurity frameworks. This finding reinforces the argument that leadership effectiveness is expressed not through isolated actions or policy declarations, but through sustained governance mechanisms that embed security into organizational decision-making.

For more detail's on strategies for Emerging technology Adoption refer to Appendix C.5 Within the framework, governance defines risk appetite, accountability, ethical alignment, and regulatory compliance. Leadership ensures that cybersecurity is treated as a strategic business concern rather than a technical function.

Technology-Specific Control Domains

Beneath the governance layer, the framework differentiates controls across AI, IoT, and Blockchain, recognizing that each technology introduces distinct risk profiles, attack surfaces, and assurance challenges.

In the case of Artificial Intelligence, the framework incorporates lifecycle-based risk management, secure MLOps practices, model governance, explainability, and protection against adversarial AI threats such as data poisoning, prompt injection, and model theft. This directly addresses the study's findings that AI-related risks often emerge due to gaps in governance rather than from the technology itself.

For IoT, the framework emphasizes architectural standardization, device-level security, supply-chain assurance, continuous monitoring, and scalability controls. These elements respond to the vulnerability patterns observed in organizations with deeper technology integration, where poorly governed IoT deployments significantly expand attack surfaces and incident likelihood.

In case of Blockchain, the framework suggests to integrate smart-contract assurance, cryptographic key management, privacy-by-design mechanisms, and immutable auditability. While blockchain inherently offers inherent integrity advantages, the study's findings and

supporting literature indicated that cybersecurity resilience depends on how governance, access control, and operational oversight are implemented within the decentralized architectures.

Proactive Hybrid Cybersecurity Framework as the Core Enabler

At the core of the unified model is the Proactive Cybersecurity Framework, which has emerged as the strongest and most statistically significant predictor of organizational resilience in the overall regression analysis. This layer synthesizes the strengths of multiple established frameworks, combining risk-based governance, secure-by-design(security-by-default) controls, threat-informed defense, and continuous risk assessment.

The framework moves beyond reactive compliance-driven security by emphasizing anticipation, adaptation, and recovery. It integrates qualitative and quantitative risk assessment, continuous monitoring, and iterative improvement, enabling organizations to evolve their security posture as emerging technologies evolve. This directly supports the study's conclusion that resilience is built through structured preparedness and governance rather than through isolated policies & approaches or increased technology investment alone.

Enterprise Information Security Outcomes

The last layer of the framework talks the desired security and resilience outcomes, including reduced incident frequency & types , lower vulnerability exposure factor, improved recovery capability, and sustained trust in emerging technology adoption. These outcomes align with the study's dependent variables and reflect the practical value of the unified framework.

Importantly, this framework explains the complex, context-dependent relationship between policy strength and resilience. Strong policies contribute positively only when embedded within proactive governance and operationalized through adaptive frameworks. Policies put in place on their own may make it harder for people to follow the rules without providing the benefits of resilience, as seen by the negative standardized coefficient for policy framework strength in the overall model.

Implications for Practice

This Unified Meta-Framework provides enterprises with a practical and evidence-based roadmap for securing emerging technologies. It recommends that organizations should prioritize

governance-driven, proactive cybersecurity capabilities over the fragmented approach focused on technology-specific solutions. By aligning leadership, frameworks, and technical controls within a single integrated model, enterprises can achieve sustainable cybersecurity resilience while continuing to innovate & grow .

In short, the suggested framework turns the study's findings and ideas into a clear recommendation, showing that strong governance and proactive measures are more important for cybersecurity resilience in new technology settings than just how much technology is used or adopted .

This Unified Meta-Framework can operationalize the empirical findings of this study.

The **governance and leadership layer** at the top explains the influence of leadership on resilience (H_o3), while the **technology-specific domains** (AI, IoT, Blockchain) reflect how deeper integration expands attack surfaces and vulnerability exposure (H_o1, H_o2). The **hybrid proactive cybersecurity framework** layer represents the strongest determinant of organizational resilience (H_o4), integrating risk-driven governance, threat-informed defense, Security-by-Design (secure-by-default), and Zero-trust principles & controls. Finally, the **outcome layer** illustrates why policy frameworks alone exhibit a complex, context-dependent relationship with resilience unless reinforced by proactive governance (H_o5).

5.6.3 Recommendations on Proactive Cybersecurity Lifecyle

The goal of a proactive framework is to **enable enterprises to innovate with adoption of emerging technologies safely.** Rather than worrying & stifling innovation, a security done right with principles like Security by Design & Default **builds trust and resilience**, allowing organizations to always reap the benefits of AI, IoT, and blockchain & any other new technology while keeping threats at bay.

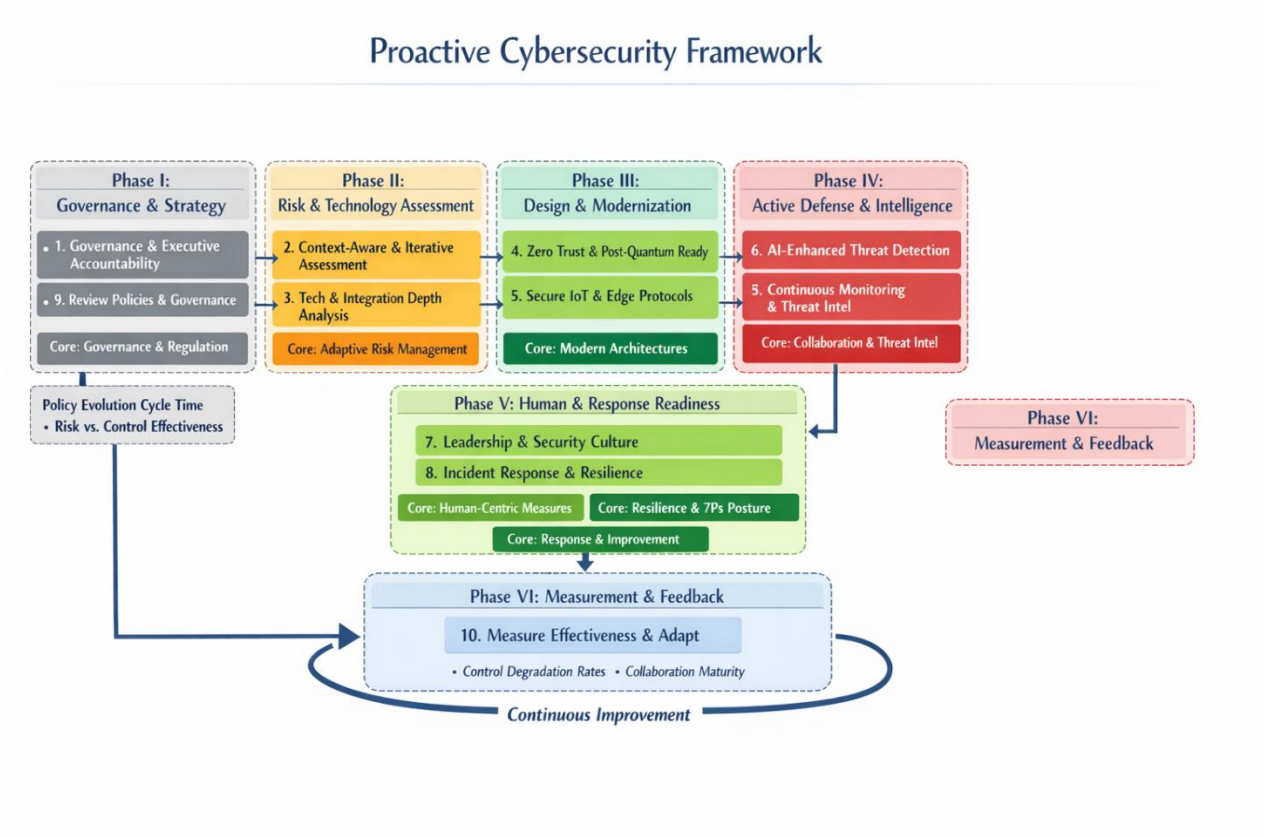


Figure 5.8

Proactive Cybersecurity Framework lifecycle

The Proactive Cybersecurity Risk Framework created integrates a 10-step lifecycle with 8 core capability domains to address emerging technology impacts and future risks.

I. The Proactive Cybersecurity Lifecycle

This 10-step continuous loop ensures that security evolves alongside technological adoption so its proactively evolving.

1. Governance & Executive Accountability - Establishes clear leadership ownership for cyber risks.

Assess Technology Adoption & Integration Depth - Evaluates how deeply new tech is embedded in the business.

2. Proactive Risk & Vulnerability Assessment - This step is focused towards Identifying weaknesses before they are exploited.

3. Security- & Privacy-by-Design Controls - This Step ensures security & protections into the initial architecture of all new systems.

4. Integrate Hybrid & Adaptive Frameworks - This step will enable the use of flexible models that combine traditional and emerging standards.

5. Continuous Monitoring & Threat Intelligence - This step is about real-time visibility into the threat landscape.

6. Strengthen Leadership & Culture - This step Fosters a security-first mindset across the entire workforce.

7. Incident Response & Resilience Planning - This step Prepares to withstand and recover from advanced attacks.

8. Review Policies & Governance - It is very important to regularly update rules to reflect new technological realities.

9. Measure Effectiveness & Adapt Continuously - define & Use metrics to refine the lifecycle and restart the process.

II. Core Capability Domains

These domains provide the technical and operational depth required to support the proactive lifecycle.

Domain no. 1 - Strategy & Governance

1. Governance & Regulation: This domain ensures to build capability through Alignment with evolving compliance standards and internal policies.
2. Adaptive Risk Management: This Domain focusses on Utilizing context-aware, iterative, and cost-sensitive prioritization for risk.
3. Collaboration & Threat Intelligence: This Domain is encourages in engaging with ecosystems and supply chains to share intelligence.

Domain no. 2 - Technical Defense & Architecture

1. Modern Architectures: This Domain encourages to adapt modern architecture like Zero Trust, post-quantum cryptography, and IoT/edge security to build defence .
2. AI-Enhanced Detection: This Domain enables enhancement detection through leveraging predictive analytics and preparing for "AI vs. AI" threats.

Domain no. 3 - Resilience & Human Factors

1. Human-Centric Measures: This domain focuses on building resilence through culture, training, and systematic error reduction.
2. Resilience & 7Ps Posture: This step helps in adopting a stance to predict, withstand, and recover from advanced threats. 7Ps Posture (Predict, Prevent, Perceive, Personalize, Prioritize, Protect, Persist) is a strategy used to predict, withstand, and recover from advanced threats , resilience is about high availability .
3. Response & Improvement: This step is about adopting tested Incident Response (IR) and continuous learning to improve outcomes.

This hierarchical flow-based model emphasizes governance-driven security, proactive risk management, and adaptive resilience. The framework reflects this study's core finding that cybersecurity resilience in emerging technology environments depends not on technology adoption alone, but on how technologies are integrated, monitored, governed, and supported through leadership and structured cybersecurity frameworks.

Table 5.4

Proactive Cybersecurity Features

Feature	Reactive (Old)	Proactively Pre-emptive (Future)
Focus	Clean-up & Recovery	Prevention & Patching --> Prediction & Auto-neutralization
Tech	Firewalls / AV	EDR / SIEM / XDR --> Agentic AI / Self-healing Infrastructure
Speed	Days / Weeks	Hours / Minutes --> Milliseconds (Real-time)
Identity	Static Passwords	Multi-factor (MFA) --> Continuous Behavioural Biometrics

5.7 Conclusions

Empirical findings from this research on emerging technology & its impact on Information security have demonstrated that any emerging technology adoption in isolation does not determine enterprise cybersecurity outcomes. Instead, the depth and planned manner of integration play a more critical role in shaping security risk. Higher levels of integration were associated with greater risks & more cybersecurity incidents, reflecting greater system complexity, more attack vectors, and a larger attack surface. A structured and formal adoption of practices was found to mitigate incident frequency, highlighting the importance of governance and disciplined implementation.

The study found that vulnerability exposure associated with the deeper integration of emerging technologies was significantly related to cybersecurity incident patterns. Vulnerabilities related to privacy, governance gaps, and implementation weaknesses have been shown to influence the types of incidents organizations experience. This confirms that vulnerability management remains a central challenge in digitally transforming enterprises. A proper, targeted & timely risk assessment covering all aspects of business would help in this case. Cybersecurity leadership was found to contribute meaningfully to organizational resilience. Strong leadership improved an organization's ability to recover from and adapt to cyber threats through process & people efficiency; however, Leadership directly did not moderate the relationship between technology integration and resilience. The findings in this research have indicated that leadership influences security outcomes primarily by enabling governance structures and strengthening cybersecurity frameworks rather than directly offsetting integration risk. Leadership is about creating actionable or tangible outcomes, so without a proactive framework, it would be hard to create/achieve a better security posture & cybersecurity resilience within the organization Among all variables examined, the proactive cybersecurity framework emerged as the strongest predictor of organizational resilience.

When the proactive framework variable was included in the regression model, it reduced the direct effect of leadership on organizational resilience. This suggested that leadership contributed to resilience only through the development and strengthening of structured Governance models & proactive, adaptable cybersecurity frameworks.

The results regarding security policies and frameworks revealed a more complex relationship. The policy framework was statistically significant, but it did not have a direct effect on incident

counts or reduce the frequency of cybersecurity incidents. This suggests that policies alone are insufficient to manage emerging technology risks unless supported by proactive frameworks, leadership engagement, and effective governance mechanisms.

Overall, the findings of this study demonstrate that effective enterprise information security management in the context of emerging technologies depends less on technology adoption itself and more or less on how these technologies are integrated, governed, and supported through leadership and structured cybersecurity frameworks. Thus, the study provides empirical evidence supporting a governance-oriented, resilience-focused approach to managing emerging technology risks and lays a foundation for both practical application and future research in enterprise information security.

Finally, it's not just for private enterprise; even integrated, proactive cybersecurity frameworks are critical for protecting national infrastructure, as adversaries consistently exploit system vulnerabilities using Emerging technologies like AI to gather intelligence before executing large-scale attacks. Technology-driven environments, such as public IP-based surveillance for Crime detection & prevention, smart power grids, Supervisory Control and Data Acquisition (SCADA) systems, and smart cities, require strong security governance embedded through security-by-design, security-by-default, privacy-by-design, zero-trust & Moving-Threat-Defence principles. A unified, proactive cybersecurity framework not only enables nations to systematically reduce exposure but also strengthens resilience and safeguards critical infrastructure against evolving, state-sponsored cyber threats & attacks.

REFERENCES

A, K.M., K, K.M. and U, K.S. (2022) 'Securing IoT devices and networks using NIST Cybersecurity Framework', *Journal of Network and Computer Applications*, 198, p.102927.

Abrahams, T.O., Farayola, Olalekan A, Kaggwa, S., Uwaoma, P.U., Hassan, A.O. and Dawodu, S.O. (2024) 'Cybersecurity awareness and education programs: A review of employee engagement and accountability', *Computer Science & IT Research Journal*, [online] 5, pp.100–119. doi:https://doi.org/10.51594/csitrj.v5i1.708.

Achuthan, K., Ramanathan, S., Srinivas, S. and Raman, R. (2024) 'Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions', *Frontiers in Big Data*, 7. doi:https://doi.org/10.3389/fdata.2024.1497535.

Adedamola Oluokun, Ige, A.B. and Ameyaw, M.N. (2024) 'Building cyber resilience in fintech through AI and GRC integration: An exploratory Study', *GSC Advanced Research and Reviews*, [online] 20, pp.228–237. doi:https://doi.org/10.30574/gscarr.2024.20.1.0245.

Ahn, S., Lee, S. and Kim, J. (2021) 'Cybersecurity risk management for artificial intelligence systems using NIST Cybersecurity Framework', *Journal of Intelligent Information Systems*, 57, pp.267–283.

Ajish, D. (2024) 'A Review on the Benefits of Continuous Threat Exposure Management in the Banking Industry', *International Journal of Current Science Research and Review*, [online] 7. doi:https://doi.org/10.47191/ijcsrr/V7-i4-21.

Akash Takyar (2023a) 'AI for regulatory compliance', [online] LeewayHertz - AI Development Company. Available at: https://www.leewayhertz.com/ai-for-regulatory-compliance/#How-does-AI-address-the-challenges-of-regulatory-compliance [Accessed Jan. 2025].

Akbar, N.A., Muneer, A., ElHakim, N. and Fati, S. (2021) 'Distributed Hybrid Double-Spending Attack Prevention Mechanism for Proof-of-Work and Proof-of-Stake Blockchain Consensuses', *Future Internet*, [online] 13, p.285. doi:https://doi.org/10.3390/fi13110285.

Akhtar, Z.B. and Ahmed, T.R. (2024) 'Enhancing Cybersecurity through AI-Powered Security

Mechanisms', *IT Journal Research and Development*, [online] 9, pp.50–67. doi:https://doi.org/10.25299/itjrd.2024.16852.

Akinsanya, O., Adebayo, O. and Oshin, O. (2024) 'Cyber resilience frameworks: Detection, response and recovery', *Journal of Information Security and Applications*, 78, p.103282. doi:https://doi.org/10.1016/j.jisa.2024.103282.

Al-Dosari, K. and Fetais, N. (2023) 'Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach', *Electronics*. [online] doi:https://doi.org/10.3390/electronics12173629.

Alshaikh, M. (2020) 'Developing cybersecurity culture to influence employee behaviour: A practice perspective', *Computers & Security*, 98, p.102003. doi:https://doi.org/10.1016/j.cose.2020.102003.

and, S. (2020) *NIST Special Publication 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations*. [online] NIST. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

and, S. (2024) 'Artificial intelligence risk management framework : generative artificial intelligence profile', [online] National Institute of Standards and Technology (U.S.). doi:https://doi.org/10.6028/NIST.AI.600-1.

Anklam, E., Bahl, M.I., Ball, R., Beger, R.D., Cohen, J., Fitzpatrick, S., Girard, P., Halamoda-Kenzaoui, B., Hinton, D., Hirose, A., Hoeveler, A., Honma, M., Hugas, M., Ishida, S., Kass, G.E., Kojima, H., Krefting, I., Liachenko, S., Liu, Y. and Masters, S. (2022) 'Emerging technologies and their impact on regulatory science', *Experimental Biology and Medicine*, [online] 247, pp.1–75. doi:https://doi.org/10.1177/15353702211052280.

Anoruo, C. (2019) 'Employing COBIT 2019 for Enterprise Governance Strategy', [online] ISACA. Available at: https://www.isaca.org/resources/news-and-trends/industry-news/2019/employing-cobit-2019-for-enterprise-governance-strategy.

Antonopoulos, A.M. (2017) *Mastering ethereum: Building smart contracts and DApps*. Sebastopol, CA: O'Reilly Media.

Aouedi, O., Vu, T.-H., Sacco, A., Nguyen, D., Piamrat, K., Marchetto, G. and Pham, V.Q. (2024) 'A Survey on Intelligent Internet of Things: Applications, Security, Privacy, and Future Directions', *IEEE Communications Surveys & Tutorials*, [online] 27, pp.1238–1292. doi:https://doi.org/10.48550/arxiv.2406.03820.

Asante, M., Epiphaniou, G., Maple, C., Al-Khateeb, H., Bottarelli, M. and Ghafoor, K. (2021) 'Distributed Ledger Technologies in Supply Chain Security Management: A Comprehensive Survey', *IEEE Transactions on Engineering Management*, [online] PP, pp.1–27. doi:https://doi.org/10.1109/tem.2021.3053655.

Assibi, A. (2023) 'Building cyber resilience capabilities: Enterprise risk management and business continuity', *Journal of Cyber Security Technology*, 7, pp.1–19. doi:https://doi.org/10.1080/23742917.2023.2201886.

Bashir, I. (2020) *MASTERING BLOCKCHAIN - THIRD EDITION : a deep dive into distributed ledgers, consensus protocols,... smart contracts, dapps, cryptocurrencies, ethereum.* Birmingham, UK: Packt Publishing Limited.

Batool, A., Zowghi, D. and Bano, M. (2025) 'AI governance: a systematic literature review', *AI and Ethics*. [online] doi:https://doi.org/10.1007/s43681-024-00653-w.

Bin, Z.Y., Ali, R., Afzal, M.K. and Kim, S.W. (2021) 'Next-Generation Internet of Things (IoT): Opportunities, Challenges, and Solutions', *Sensors*, 21, p.1174. doi:https://doi.org/10.3390/s21041174.

Bitdefender (2025) 'The 2025 IoT Security Landscape Report', [online] Available at: https://blogapp.bitdefender.com/hotforsecurity/content/files/2025/10/2025_iot_security_report.pdf Viewed 24 Jan 2026.

Björn, L. and Niklas, M. (2019) 'Defining Information Security', [online] philpapers.org. Available at: https://philpapers.org/rec/LUNDIS-2.

Bonderud, D. (2024) 'Cost of a data breach in 2024 for the financial industry', [online] IBM. Available at: https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry.

California, A. and Ajish, D. (2024) 'A Review on the Benefits of Continuous Threat Exposure Management in the Banking Industry', *International Journal of Current Science Research and Review*, [online] 07. doi:https://doi.org/10.47191/ijcsrr/V7-i4-21.

Campbell, S. (2020) 'Quantum computing and the need for quantum resistant solutions', *International Journal of Quantum Information*, 18, p.2050046. doi:https://doi.org/10.1142/S021974992050046X.

Chegini, H., Naha, R.K., Mahanti, A. and Thulasiraman, P. (2021) 'Process Automation in an IoT–Fog–Cloud Ecosystem: A Survey and Taxonomy', *IoT*, 2, pp.92–118. doi:https://doi.org/10.3390/iot2010006.

Chen, L., Chen, P. and Lin, Z. (2020) 'Artificial Intelligence in Education: a Review', *IEEE Access*, [online] 8, pp.75264–75278. doi:https://doi.org/10.1109/ACCESS.2020.2988510.

Cheng, X. (2023) 'The Widespread Application of Artificial Intelligence in Education Necessitates Critical Analyses', *Science Insights Education Frontiers*. [online] doi:https://doi.org/10.15354/sief.23.co081.

Chu, H., Zhang, P., Dong, H., Xiao, Y., Ji, S. and Li, W. (2023) 'A survey on smart contract vulnerabilities: Data sources, detection and repair', *Inf. Softw. Technol.*, [online] 159, p.107221. doi:https://doi.org/10.1016/j.infsof.2023.107221.

Cloudsecurityalliance.org. (2025) 'AI Controls Matrix | Framework for Trustworthy AI | CSA', [online] Available at: https://cloudsecurityalliance.org/artifacts/ai-controls-matrix [Accessed Jan. 2025].

cloudsecurityalliance.org. (2022) 'IoT Security Controls Framework v3 | CSA', [online] Available at: https://cloudsecurityalliance.org/artifacts/iot-security-controls-framework-v3 [Accessed Jan. 2024].

Coherent Solutions (2025) '2025 AI Adoption Across Industries: Trends You Don’t Want to Miss', [online] Coherentsolutions.com. Available at: https://www.coherentsolutions.com/insights/ai-adoption-trends-you-should-not-miss-2025 [Accessed Jan. 2025].

Collum, C. and Kettani, H. (2022) 'On Security Implications of Emerging Technologies', *2022 3rd International Conference on Education Development and Studies*, 1. doi:https://doi.org/10.1145/3528137.3528159.

Common guideposts to promote interoperability in AI risk management (2023) doi:https://doi.org/10.1787/ba602d18-en.

ConsenSys Diligence (2023) 'A guide to smart contract security best practices', [online] Available at: https://consensysdiligence.github.io/smart-contract-best-practices/attacks/.

Copado, T. (2022) 'DIE Model Security vs. the CIA Security Triad | Copado', [online] Available at: https://www.copado.com/resources/blog/making-die-model-security-vs-the-cia-security-triad-complementary-not-competitive [Accessed Apr. 2024].

CrowdStrike (2025) '2025 Global Threat Report', [online] Available at: https://www.crowdstrike.com/en-us/global-threat-report/ Accessed 24 Jan 2026.

Dahmer, J. (2020) 'Organizational culture and cybersecurity: The role of project managers', *Information & Computer Security*, 28, pp.727–743. doi:https://doi.org/10.1108/ICS-05-2020-0082.

Davies, J. (2024) 'Enhanced scalability and privacy for blockchain data using Merklized transactions', *Frontiers Blockchain*, [online] 6. doi:https://doi.org/10.3389/fbloc.2023.1222614.

Deloitte (2025) 'Cybersecurity Report 2025: AI Threats, Email Server Security, and Advanced Threat Actors', [online] Available at: https://www.deloitte.com/us/en/services/consulting/articles/cybersecurity-report-2025.html Accessed 24 Jan 2026.

Devasia, A. (2025) 'AI Cyber Threat Statistics: The 2025 Landscape of AI-Powered Cyberattacks', [online] Available at: https://thenetworkinstallers.com/blog/ai-cyber-threat-statistics/ Accessed 24 Jan 2026.

Donalds, C. and Osei-Bryson, K.-M. (2020) 'Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents', *International Journal of*

Information Management, [online] 51, p.102056. doi:https://doi.org/10.1016/j.ijinfomgt.2019.102056.

E, A.E., Chukwuba, K., S, T.A. and Ekpobimi, H. (2025) 'Transformational leadership and cyber-security innovation: How visionary leaders drive technological progress and security', *International Journal of Multidisciplinary Research and Growth Evaluation*, 6, pp.1729–1742.

Espíndola, O.R., Chowdhury, S., Dey, P.K., Albores, P. and Emrouznejad, A. (2022) 'Analysis of the adoption of emergent technologies for risk management in the era of digital manufacturing', *Technological Forecasting and Social Change*, [online] 178, p.121562. Available at: https://www.sciencedirect.com/science/article/pii/S0040162522000944.

Esther, O.A., Alabdulatif, A., Isaac, A.O., Alawida, M., Alabdulatif, A., Hamdan, A.W. and Arshad, H. (2021) 'THE INTERNET OF THINGS SECURITY: A SURVEY ENCOMPASSING UNEXPLORED AREAS AND NEW INSIGHTS', *Computers & security*. [online] doi:https://doi.org/10.1016/J.COSE.2021.102494.

F, S.M., Lubis, M. and Fakhrurroja, H. (2023) 'Counterattacking cyber threats: A framework for the future of cybersecurity', *Sustainability*, 15, p.13369.

Fang, X., Misra, S., Xue, G. and Yang, D. (2012) 'Smart Grid — The New and Improved Power Grid: A Survey', *IEEE Communications Surveys & Tutorials*, 14, pp.944–980. doi:https://doi.org/10.1109/surv.2011.101911.00087.

Farayola, O. (2024) 'AI, blockchain, and business intelligence: Revolutionizing security in the banking sector', *Journal of Financial Crime*, 31, pp.177–194. doi:https://doi.org/10.1108/JFC-01-2023-0012.

Fla, O. (2025) 'Gartner Identifies the Top Strategic Technology Trends for 2026', Gartner.

Fortinet (2024) 'What is hardware security module (HSM)?', [online] Available at: https://www.fortinet.com/resources/cyberglossary/hardware-security-module.

Fuchs, D., Kuys, B., Eisenbart, B. and Gericke, K. (2025) 'A systematic literature review on emerging technology risks in Industry 4.0/5.0: identification, clustering and developing

mitigation strategies', *Proceedings of the Design Society*, 5, pp.299–308. doi:https://doi.org/10.1017/pds.2025.31.

Giudici, P., Mattia Centurelli and Turchetta, S. (2024) 'Artificial Intelligence risk measurement', *Expert Systems with Applications*, 235, pp.121220–121220. doi:https://doi.org/10.1016/j.eswa.2023.121220.

Godulla, A., Hoffmann, C.P. and Seibert, D. (2021) 'Dealing with deepfakes – an interdisciplinary examination of the state of research and implications for communication studies', *Studies in Communication and Media*, 10, pp.72–96. doi:https://doi.org/10.5771/2192-4007-2021-1-72.

Goundar, S. and Gondal, I. (2025) 'AI-Blockchain Integration for Real-Time Cybersecurity: System Design and Evaluation', *Journal of Cybersecurity and Privacy*, 5, p.59.

Gragg, J. (2022) 'NIST RMF: A Framework for Managing Risk in Enterprise Technology', *Journal of Information Systems Security*, 22, pp.1–12.

Habbal, A., Ali, M.K. and Ali, A.M. (2024) 'Artificial Intelligence Trust, Risk and Security Management (AI TRiSM): Frameworks, applications, challenges and future research directions', *Expert Systems with Applications*, [online] 240. doi:https://doi.org/10.1016/j.eswa.2023.122442.

Hasan, M.K., Alkhalifah, A., Islam, S., Babiker, Nissrein B. M, Habib, Aman, and Hossain, M.A. (2022) 'Blockchain Technology on Smart Grid, Energy Trading, and Big Data: Security Issues, Challenges, and Recommendations', *Wireless Communications and Mobile Computing*, [online] 2022, p.e9065768. doi:https://doi.org/10.1155/2022/9065768.

Hassan, K. (2025) 'AI Cyber Attack Statistics 2025: Trends, Costs, Defense', [online] Available at: https://deepstrike.io/blog/ai-cyber-attack-statistics-2025 [Accessed Dec. 2025]. Accessed 24 Jan 2026.

Hausken, K. (2020) 'Cyber resilience strategies for societal actors', *International Journal of Critical Infrastructure Protection*, 31, p.100392. doi:https://doi.org/10.1016/j.ijcip.2020.100392.

https://www.etsi.org/. (2024) 'CYBER; Cyber Security for Consumer Internet of Things:

Baseline Requirements', [online] Available at: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/03.01.01_60/ts_103645v030101p.pdf [Accessed Jan. 2025].

Hu, Y., Kuang, W., Qin, Z., Li, K., Zhang, J., Gao, Y., Li, W. and Li, K. (2021) 'Artificial Intelligence Security: Threats and Countermeasures', *ACM Computing Surveys*, 55, pp.1–36. doi:https://doi.org/10.1145/3487890.

Hussain, F., Hussain, R., A, H.S. and Hossain, E. (2020) 'Machine Learning in IoT Security: Current Solutions and Future Challenges', *IEEE Communications Surveys Tutorials*, [online] 22, pp.1686–1721. doi:https://doi.org/10.1109/COMST.2020.2986444.

IEEE standard for an architectural framework for the internet of things (IoT). (2020) *IEEE Std 2413-2019*, pp.1–269. doi:https://doi.org/10.1109/IEEESTD.2020.9032420.

Institute, F. (2023) 'The Importance and Effectiveness of Quantifying Cyber Risk', [online] www.fairinstitute.org. Available at: https://www.fairinstitute.org/fair-risk-management.

Intelligence, D. (2025) 'IoT Hacking Statistics 2025: Threats, Risks & Regulations', [online] Available at: https://deepstrike.io/blog/iot-hacking-statistics Viewed 24 Jan 2026.

Investopedia (2025) 'Understanding proof-of-stake: How PoS transforms cryptocurrency', [online] Available at: https://www.investopedia.com/terms/p/proof-stake-pos.asp.

Ioannidis, J., Harper, J., Quah, M.-S. and Hunter, D. (2023) 'Gracenote.ai: Legal Generative AI for Regulatory Compliance', *LegalAIIA@ICAIL*. [online] doi:https://doi.org/10.2139/SSRN.4494272.

Ivanov, N., Li, C., Yan, Q., Sun, Z.-G., Cao, Z. and Luo, X. (2023) 'Security Threat Mitigation for Smart Contracts: A Comprehensive Survey', *ACM Computing Surveys*, [online] 55, pp.1–37. doi:https://doi.org/10.1145/3593293.

Joyce, S. (2023) 'The C-suite playbook: Putting security at the epicenter of innovation Findings from the 2024 Global Digital Trust Insights', [online] PwC US. Available at: https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-

digital-trust-insights/pwc-2024-global-digital-trust-insights-main-report.pdf [Accessed Jan. 2023].

Juliana, T.O., Adesokan-Imran, Temilade Oluwatoyin, Comfort, B.D., Salami, I.A., Onyenaucheya, Ogechukwu Scholastica and Olaniyi, O. (2025) 'Improving Patient Data Privacy and Authentication Protocols against AI-Powered Phishing Attacks in Telemedicine', *Asian Journal of Research in Computer Science*. [online] doi:https://doi.org/10.9734/ajrcos/2025/v18i4610.

Jyoti, R. (2023) 'White Paper Why AI Governance Is a Business Imperative for Scaling Enterprise Artificial Intelligence SITUATION OVERVIEW According to IDC's Worldwide Semiannual Artificial Intelligence Systems Spending Guide, version 1', [online] Available at: https://www.ibm.com/downloads/cas/KXVRM5QE [Accessed Mar. 2024].

Kahnke, B. (2024) 'Data Quality Is Now The Primary Factor Limiting GenAI Adoption', [online] Forrester. Available at: https://www.forrester.com/blogs/gen-ai-data-quality-b2b/ [Accessed Jan. 2024].

Kamuangu, P. (2024) 'A review on cybersecurity in fintech: Threats, solutions, and future trends', *Journal of Economics, Finance and Accounting Studies*, 6, pp.1–15.

Kanaan, A., H, A.A., Alorfi, A. and Aloun, M. (2024) 'Cybersecurity resilience for business: a comprehensive model for proactive defence and swift recovery', IEEE, pp.1–7.

kanpur, I. (2023) 'Cybersecurity Trends: Emerging Threats and Technologies in the Cybersecurity Landscape - IFACET', [online] ifacet.iitk.ac.in. Available at: https://ifacet.iitk.ac.in/knowledge-hub/cyber-security/cybersecurity-trends-emerging-threats-and-technologies-in-the-cybersecurity-landscape/ [Accessed Jan. 2024].

Karie, N.M., Masri, S.N. and Haskell-Dowland, P. (2020) 'IoT Threat Detection Advances, Challenges and Future Directions', *IEEE Xplore*. [online] doi:https://doi.org/10.1109/ETSecIoT50046.2020.00009.

Kaur, G., Lashkari, Zahra H and Lashkari, A.H. (2021) 'Cybersecurity risk in FinTech', Springer, pp.21–40.

Kaur, R., Gabrijelčič, D. and Klobučar, T. (2023) 'Artificial intelligence for cybersecurity: Literature review and future research directions', *Information Fusion*, [online] 97, p.101804. doi:https://doi.org/10.1016/j.inffus.2023.101804.

Kayode-Ajala, O. (2023) 'Applications of Cyber Threat Intelligence (CTI) in Financial Institutions and Challenges in Its Adoption', *Applied Research in Artificial Intelligence and Cloud Computing*, [online] 6, pp.1–21. Available at: https://researchberg.com/index.php/araic/article/view/159/152 [Accessed Jan. 2023].

KELA Research (2025) '2025 AI Threat Report: How cybercriminals are weaponizing AI technology', [online] KELA. Available at: https://info.ke-la.com/hubfs/Reports/KELA%20Report%20-%202025%20AI%20Threat%20Report.pdf Accessed 24 Jan 2026.

Kim, J., Lee, S. and Ahn, S. (2021) 'Identifying and mitigating cybersecurity risks using NIST Cybersecurity Framework', *Journal of Cybersecurity*, 7, pp.1–15.

Komalavalli, C., Saxena, D., Laroiya, C., Krishnan, S., Balas, V.E., Golden, J.E., Harold, R.Y., Balaji, S. and Kumar, R. (2020) 'Chapter 14 - Overview of Blockchain Technology Concepts', [online] ScienceDirect. Available at: https://www.sciencedirect.com/science/article/abs/pii/B9780128198162000149.

Kumar, O'Brien, D.R., Albert, K., Viljöen, S. and Snover, J. (2019) 'Failure Modes in Machine Learning Systems', [online] Available at: https://dblp.uni-trier.de/db/journals/corr/corr1911.html#abs-1911-11034.

Kumar, S. and Mallipeddi, Rakesh R (2022) 'Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions', *Production and Operations Management*, 31. doi:https://doi.org/10.1111/poms.13859.

Kuznetsov, O., Yezhov, A., Yusiuk, V. and Kuznetsova, K. (2024) 'Scalable Zero-Knowledge Proofs for Verifying Cryptographic Hashing in Blockchain Applications', [online] arXiv.org. Available at: https://arxiv.org/abs/2407.03511 [Accessed Jan. 2025].

Kuznetsov, S., Sernani, P., Romeo, L., Frontoni, E. and Mancini, A. (2023) 'On the Integration

of Artificial Intelligence and Blockchain Technology: A Perspective About Security', *IEEE Access*, 11, pp.137351–137367. doi:https://doi.org/10.1109/ACCESS.2023.3349019.

Lacoma, T. (2025) 'Smart Device Cyberattacks More Than Doubled in 2024', [online] CNET. Available at: https://www.cnet.com/home/security/smart-device-cyberattacks-more-than-doubled-in-2024-should-you-worry/ Viewed 24 Jan 2026.

Lalla, V., Mitrani, A. and Harned, Z. (2022) 'Artificial intelligence: deepfakes in the entertainment industry', [online] www.wipo.int. Available at: https://www.wipo.int/wipo_magazine/en/2022/02/article_0003.html.

Lee, S., Kim, J. and Ahn, S. (2022) 'Improving cybersecurity risk management practices using NIST Cybersecurity Framework', *Journal of Information Security*, 13, pp.157–171.

Lee, S., Perera, H., Xia, B., Liu, Y., Lu, Q., Zhu, L., Salvado, O. and Whittle, J. (2023) 'QB4AIRA: A QUESTION BANK FOR AI RISK ASSESSMENT', [online] Available at: https://arxiv.org/pdf/2305.09300 [Accessed Apr. 2024].

Lewallen, J. (2020) 'Emerging Technologies and Problem Definition uncertainty: the Case of Cybersecurity', *Regulation & Governance*, 15. doi:https://doi.org/10.1111/rego.12341.

Li, P. and Zhang, L. (2025) 'Application of big data technology in enterprise information security management', *Scientific Reports*, [online] 15. doi:https://doi.org/10.1038/s41598-025-85403-6.

Li, Y. and Liu, Q. (2021) 'A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments', *Energy Reports*, [online] 7, pp.8176–8186. doi:https://doi.org/10.1016/j.egyr.2021.08.126.

Linkov, I., Trump, B.D., Poinsatte-Jones, K. and V, Florin M (2018) 'Governance of emerging technologies: resilience, risk, and socio-technical systems', *Risk Analysis*, 38, pp.2494–2507. doi:https://doi.org/10.1111/risa.13204.

Liu, E., Cai, Z., Ye, Y., Zhou, M., Liao, H. and Yi, Y. (2023) 'An Overview of Flexible Sensors: Development, Application, and Challenges', *Sensors*, 23, p.765. doi:https://doi.org/10.3390/s23020765.

Loonam, J., Eaves, S., Kumar, V. and Parry, G.C. (2020) 'Towards digital transformation: Lessons learned from traditional organizations', *Strategic Change*, 29, pp.461–469. doi:https://doi.org/10.1002/jsc.2359.

Loonam, J., O'Brien, C. and Corcoran, P. (2020) 'Strategic leadership for cybersecurity: Fostering a culture of cyber resilience', *Information & Computer Security*, 28, pp.683–703. doi:https://doi.org/10.1108/ICS-05-2020-0078.

Lori Perri (2023) 'What It Takes to Make AI Safe and Effective', [online] Available at: https://www.gartner.com/en/articles/what-it-takes-to-make-ai-safe-and-effective.

Macedo, de, Silva, F.H., Mello, R.R., Felipe, Delicato, F.C., de and de (2019) 'On the security aspects of Internet of Things: A systematic literature review', *Journal of Communications and Networks*, [online] 21, pp.444–457. doi:https://doi.org/10.1109/JCN.2019.000048.

Mahbooba, B., Timilsina, M., Sahal, R. and Serrano, M. (2021) 'Explainable Artificial Intelligence (XAI) to Enhance Trust Management in Intrusion Detection Systems Using Decision Tree Model', *Complexity*, 2021, pp.1–11. doi:https://doi.org/10.1155/2021/6634811.

Malatji, M. and Tolah, A. (2024) 'Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI', *AI and Ethics*. [online] doi:https://doi.org/10.1007/s43681-024-00427-4.

Malhotra, P., Singh, Y., Anand, P., Kumar, B.D., Singh, P.K. and Hong, W.-C. (2021) 'Internet of Things: Evolution, Concerns and Security Challenges', *Sensors*, [online] 21, p.1809. doi:https://doi.org/10.3390/s21051809.

Manu, A. (2024) *Generative AI as a Disruptor*. Boca Raton, FL: Chapman and Hall/CRC.

Mbah, O. and Nkechi, E. (2024) 'AI-driven threats and data protection regulations: Balancing innovation and compliance', *Journal of Information Privacy and Security*, 20, pp.22–38. doi:https://doi.org/10.1080/15536548.2024.2307890.

Melaku, H.M. (2023) 'Context-Based and Adaptive Cybersecurity Risk Management Framework', *Risks*, [online] 11, p.101. Available at: https://www.mdpi.com/2227-9091/11/6/101.

Mızrak, F. (2023) 'Integrating cybersecurity risk management into strategic management: a comprehensive literature review', *Journal of Business, Economics and Finance*, 10. doi:https://doi.org/10.17261/pressacademia.2023.1807.

Mohammed, M.M., Li, Y. and Meheretie, D.L. (2021) 'A survey on internet of energy security: related fields, challenges, threats and emerging technologies', *Cluster Computing*, 15. doi:https://doi.org/10.1007/s10586-021-03423-z.

Mougayar, W. (2015) 'Understanding the blockchain', [online] O'Reilly Media. Available at: https://www.oreilly.com/radar/understanding-the-blockchain/ [Accessed Apr. 2024].

Mouha, Radouan Ait (2021) 'Internet of Things (IoT)', *Journal of Data Analysis and Information Processing*, [online] 9, pp.77–101. doi:https://doi.org/10.4236/jdaip.2021.92006.

Mrabet, H., Belguith, S., Alhomoud, A. and Jemai, A. (2020) 'A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis', *Sensors*, 20, p.3625. doi:https://doi.org/10.3390/s20133625.

Mueller, G.B., Jensen, B., Valeriano, B., Maness, R.C. and Macias, J.M. (2023) 'Cyber Operations during the Russo-Ukrainian War', *www.csis.org*, [online] 2023. Available at: https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war#:~:text=Of%20the%2030%20recorded%20cyber.

Murugesan, U., Subramanian, P., Srivastava, S. and Dwivedi, A. (2023) 'A study of Artificial Intelligence impacts on Human Resource Digitalization in Industry 4.0', *Decision Analytics Journal*, [online] 7, p.100249. doi:https://doi.org/10.1016/j.dajour.2023.100249.

Nakamoto, S. (2008) 'Bitcoin: A Peer-to-Peer Electronic Cash System'. [online] doi:https://doi.org/10.2139/SSRN.3440802.

Narayanan, A., Clark, J. and Kroll, J. (2016) *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton, NJ: Princeton University Press.

NIST, G.M. (2024a) 'NIST Cybersecurity Framework 2.0:', [online] doi:https://doi.org/10.6028/NIST.SP.1300.SPA.

NIST, G.M. (2024b) 'The NIST Cybersecurity Framework (CSF) 2.0 (French translation)'. [online] doi:https://doi.org/10.6028/NIST.CSWP.29.FRE.

Obiki-Osafiele, Amara N, Agu, E.E. and Chiekezie, Nkiru R (2024) 'Protecting digital assets in fintech: Essential cybersecurity measures and best practices', *Computer Science & IT Research Journal*, 12, pp.1884–1896.

ODoherty, C. (2023) 'Emerging Technologies And Their Impact On Cyber Security', [online] www.metacompliance.com. Available at: https://www.metacompliance.com/blog/cyber-security-awareness/emerging-technologies-and-their-impact.

OECD (2026) 'Emerging Technologies', [online] Available at: https://www.oecd.org/en/topics/emerging-technologies.html Viewed 24 Jan 2026.

Okolo, F., Tsekiri, A. and Sydney, A.A. (2024) 'Security Awareness Programs and Behavioral Patterns in Nigeria Deposit Money Banks: Adopting a Robust Cybersecurity Culture', *International Journal of Research and Innovation in Social Science*, [online] VIII, pp.239–256. doi:https://doi.org/10.47772/IJRISS.2024.806019.

Oluokun, None Adedamola, Ige, B. and Nana, M. (2024) 'Building cyber resilience in fintech through AI and GRC integration: An exploratory Study', *GSC Advanced Research and Reviews*, [online] 20, pp.228–237. doi:https://doi.org/10.30574/gscarr.2024.20.1.0245.

Osmani, Z. (2023) 'GLOBAL LONG-TERM UNCONSTRAINED SEISMIC CHANGES FROM ARTIFICIAL INTELLIGENCE A quality growth opportunity', [online] Martin Currie Investment Management Limited. Available at: https://www.martincurrie.com/__data/assets/pdf_file/0022/44608/Martin-Currie-GLTU-AI-Seismic-Change-Nov-23.pdf [Accessed Jan. 2024].

OWASP (2018) 'OWASP Internet of Things Project - OWASP', [online] wiki.owasp.org. Available at: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10.

owasp.org. (2025) 'OWASP Smart Contract Top 10 | OWASP Foundation', [online] Available at: https://owasp.org/www-project-smart-contract-top-10/.

Parker, S. and Bach, C. (2020) 'Blockchain, AI, and IoT: Transforming information access and security', *Information Technology & People*, 33, pp.1709–1731. doi:https://doi.org/10.1108/ITP-01-2019-0012.

Parsanna, M. (2025) 'A Review on Various Machine Learning Algorithms', *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*. [online] doi:https://doi.org/10.55041/ijsrem42692.

Parums, D.V. (2021) 'Editorial: Review Articles, Systematic Reviews, Meta-Analysis, and the Updated Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 Guidelines', *Medical Science Monitor*, [online] 27. doi:https://doi.org/10.12659/msm.934475.

Patricia, O., Adesoga, Taiwo O, Ojo, A., Olagunju, Olaseni D, Ajayi, O.O. and Adebayo, Y.O. (2024) 'Cybersecurity strategies in fintech: Safeguarding financial data and assets', *GSC Advanced Research and Reviews*, [online] 20, pp.1–10. doi:https://doi.org/10.30574/gscarr.2024.20.3.0123.

Porter, J. (2025) 'Emerging Technology: What It Is, Why It Matters, and How It's Transforming 2025', [online] The London Report. Available at: https://thelondonreport.co.uk/technology/emerging-technology/ Viewed 24 Jan 2026.

Potter, K., d, lucas and Oloyede, J. (2023) 'The Internet of Things: Transforming Industries, Empowering Connectivity, and Shaping the Future', *Journal on Internet of Things*.

PricewaterhouseCoopers (2023a) 'Cybersecurity + geopolitical conflict: What boards and CEOs should know and act upon', [online] PwC. Available at: https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/cybersecurity-geopolitical-conflict-board-ceo-response.html.

PricewaterhouseCoopers (2023b) 'Digital Trust Insights 2023', [online] PwC. Available at: https://www.pwc.com/ng/en/publications/global-digital-trust-insights.html.

Project Management Institute (2019) *The standard for risk management in portfolios, programs, and projects*. Newtown Square, PA: Project Management Institute.

Raban, Y. and Hauptman, A. (2018) 'Cyber resilience: Attack and defense capabilities', *Journal of Information Warfare*, 17, pp.1–13.

Radanliev, P. (2024) 'AI and blockchain: New risks and vulnerabilities in the internet of things', *Internet Technology Letters*, 7, p.e699. doi:https://doi.org/10.1002/itl2.699.

Rao, K. (2022) *Design of Internet of Things*. Boca Raton, FL: CRC Press.

Rasmussen, R. and Hougan, M. (2024) 'Crypto Use Cases 2024 12 Real-World Stories of How Millions of People Are Using Crypto Services Today', [online] bitwise. Available at: https://s3.amazonaws.com/static.bitwiseinvestments.com/Research/Crypto-Use-Cases-12-Real-World-Stories-2024.pdf [Accessed Jan. 2024].

Reddy, R.P. (2024) 'The Rise of AI-powered Cybercrime: a Data-driven Analysis of Emerging Threats', *International Journal For Multidisciplinary Research*. [online] doi:https://doi.org/10.36948/ijfmr.2024.v06i06.30744.

Research, Kaspersky Global and Team, A. (2025) 'Mirai Botnet Targeting IoT Devices: 2024–2025 Threat Update', [online] Available at: https://me-en.kaspersky.com/about/press-releases/kaspersky-discovers-multiple-iot-devices-targeted-with-a-new-mirai-botnet-version Viewed 24 Jan 2026.

Research, A. (2025) 'IoT Security Breaches Report: Original Data & Industry Insights 2025', [online] Available at: https://acsmi.org/blogs/iot-security-breaches-report-original-data-amp-industry-insights-2025 Viewed 24 Jan 2026.

Revelo (2023) 'What is blockchain in cloud computing?', [online] Available at: https://www.revelo.com/blog/blockchain-cloud-computing.

Rochman, K. and Sanjaya, I. (2022) *International Journal of Current Science Research and Review*.

Rotolo, D., Hicks, D. and Martin, B. (2015) 'What Is an Emerging Technology?', [online] arXiv. Available at: https://arxiv.org/pdf/1503.00673v1 Viewed 24 Jan 2026.

S, Maheswari U (2024) 'Cybersecurity challenges in fintech: Assessing threats and mitigation strategies for financial institutions', *Educational Administration: Theory and Practice*, 30, pp.1–15.

S, R.R., Y, P.V., Dempsey, K., Ransom, M. and O'Neill, M. (n.d.) 'NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations', *Journal of Cybersecurity*, [online] 8, pp.1–17. doi:https://doi.org/10.1093/cybsec/tyac001.

Saeed, S., Altamimi, S.A., Alkayyal, N.A., Alshehri, E. and Alabbad, D.A. (2023) 'Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations', *Sensors*, 23, p.6623. doi:https://doi.org/10.3390/s23156623.

Salah, K., Rehman, Nizamuddin, N. and Al-Fuqaha, A. (2019) 'Blockchain for AI: Review and Open Research Challenges', *IEEE Access*, [online] 7, pp.10127–10149. doi:https://doi.org/10.1109/access.2018.2890507.

Salama, R., Altrjman, C. and Al-Turjman, F. (2024) 'An overview of future cybersecurity applications using AI and blockchain technology', *Computational intelligence and blockchain in complex systems*, pp.1–11.

Saleh, (2024) 'Blockchain for secure and decentralised artificial intelligence in cybersecurity: A comprehensive review', *Blockchain: Research and Applications*, 5, p.100193.

Samonas, S. and Coss, D. (2014) 'The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security'.

Sangwan, Raghvinder S, Badr, Y. and Srinivasan, S.M. (2023) 'Cybersecurity for AI Systems: A Survey', *Journal of Cybersecurity and Privacy*, 3, pp.166–190. doi:https://doi.org/10.3390/jcp3020010.

Santos-Olmo, A., Sánchez, L., Rosado, D., Serrano, M., Blanco, C., Mouratidis, H. and Fernández-Medina, E. (2023) 'Towards an integrated risk analysis security framework according to a systematic analysis of existing proposals', *Frontiers of Computer Science*, [online] 18, pp.1–18. doi:https://doi.org/10.1007/s11704-023-1582-6.

Sarkis, A. (2023) *Training Data for Machine Learning*. Sebastopol, CA: 'O'Reilly Media, Inc.'

Sayeed, S., Marco-Gisbert, H. and Caira, T. (2020) 'Smart Contract: Attacks and Protections', *IEEE Access*, [online] 8, pp.24416–24427. doi:https://doi.org/10.1109/access.2020.2970495.

Schmitt, M. (2023) 'Securing the digital world: Protecting smart infrastructures and digital industries with artificial-intelligence-enabled malware and intrusion detection', *Journal of Industrial Information Integration*, 32, p.100420. doi:https://doi.org/10.1016/j.jii.2022.100420.

Schuett, J. (2022) 'Defining the scope of AI regulations', *arXiv*. [online] doi:https://doi.org/10.48550/arXiv.1909.01095.

Security by Design for IoT Device Manufacturers ISO 9001 :2015 TECHNICAL REPORT TEC 31328:2023. (2023) MINISTRY OF COMMUNICATIONS GOVERNMENT OF INDIA.

Shankar, R., Kumar, S., David, O., Albertˆ, K., Viljoen, S., Snover, J. and Microsoft (2019) 'Failure Modes in Machine Learning', [online] arXiv. Available at: https://arxiv.org/ftp/arxiv/papers/1911/1911.11034.pdf.

Sharma, P., Singh, S. and Kumar, N. (2020) 'Cloud security using NIST Cybersecurity Framework', *Journal of Cloud Computing*, 9, pp.1–15.

Shinde, P., Kolhe, S., Pawar, A. and Katti, V. (2021) 'Blockchain and artificial intelligence in cybersecurity: A review and future research directions', *Journal of Open Innovation: Technology, Market, and Complexity*, 7, p.188. doi:https://doi.org/10.3390/joitmc7030188.

Simona-Nicoleta Vulpe, Răzvan Rughiniș, Dinu Țurcanu and Rosner, D. (2024) 'AI and cybersecurity: a risk society perspective', *Frontiers in Computer Science*, 6. doi:https://doi.org/10.3389/fcomp.2024.1462250.

Singh, M. and Kim, S. (2019) 'Blockchain technology for decentralized autonomous organizations', *Advances in Computers*, [online] 115, pp.115–140. doi:https://doi.org/10.1016/bs.adcom.2019.06.001.

Singh, S., Sanwar Hosen, A.S.M and Yoon, B. (2021) 'Blockchain Security Attacks, Challenges,

and Solutions for the Future Distributed IoT Network', *IEEE Access*, 9, pp.1–1. doi:https://doi.org/10.1109/access.2021.3051602.

Smetanin, S., Ometov, A., Komarov, M., Masek, P. and Koucheryavy, Y. (2020) 'Blockchain Evaluation Approaches: State-of-the-Art and Future Perspective', *Sensors*, 20, p.3358. doi:https://doi.org/10.3390/s20123358.

SonicWall (2024) '2024 Mid-Year Cyber Threat Report', [online] Available at: https://wca.org/security-attacks-on-iot-devices-surge-by-107-in-early-2024/ Viewed 24 Jan 2026.

SonicWall (2025) '2025 Annual Cyber Threat Report', [online] Available at: https://www.cnet.com/home/security/smart-device-cyberattacks-more-than-doubled-in-2024-should-you-worry/ Viewed 24 Jan 2026.

Spencer-Hicken, S., Schutte, and J, V.P. (2023) 'Blockchain feasibility assessment: A quantitative approach', *Frontiers in Blockchain*, 6. doi:https://doi.org/10.3389/fbloc.2023.1067039.

Stahl, B.C. and Eke, D. (2024) 'The ethics of ChatGPT – Exploring the ethical issues of an emerging technology', *International Journal of Information Management*, [online] 74, p.102700. doi:https://doi.org/10.1016/j.ijinfomgt.2023.102700.

Startup Defense (2023) 'Eclipse attack defense guide for blockchain networks', [online] Available at: https://www.startupdefense.io/cyberattacks/eclipse-attack.

Sultana, N., A, N.M., Majumder, C. and Choain, A. H. K (2024) 'Exploring AI-Driven Approaches for Safeguarding Sensitive ERP, HR, and Defence Data within US Organisations', *Journal of Business Insight and Innovation*, 3, pp.43–59.

Sutton, A. and Tompson, L. (2024) 'Towards a cybersecurity culture-behaviour framework: A rapid evidence review', *Computers & Security*, 139, p.103698. doi:https://doi.org/10.1016/j.cose.2023.103698.

T, H.S., Yigitcanlar, T., Nguyen, K. and Xu, Y. (2024) 'Understanding local government cybersecurity policy: A concept map and framework', *Information*, 15, p.342.

Takyar, A. (2023b) 'AI for regulatory compliance', [online] Available at: https://www.leewayhertz.com/ai-for-regulatory-compliance/#How-does-AI-address-the-challenges-of-regulatory-compliance [Accessed Jan. 2025].

Tariq, U., Ahmed, I., Bashir, A.K. and Shaukat, K. (2023) 'A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review', *Sensors*, 23. doi:https://doi.org/10.3390/s23084117.

Team, N.S. (2024) 'The 2024 IoT Security Landscape Report', [online] Available at: https://www.netgear.com/hub/network/2024-iot-threat-report/ Viewed 24 Jan 2026.

Theobald, O. (2024) *AI FOR ABSOLUTE BEGINNERS*. Birmingham, UK: Packt Publishing Ltd.

ThreatLabz, Z. (2025a) '2025 Mobile, IoT & OT Threat Report', [online] Available at: https://www.zscaler.com/blogs/security-research/industry-attacks-surge-mobile-malware-spreads-threatlabz-2025-mobile-iot-ot Viewed 24 Jan 2026.

ThreatLabz, Z. (2025b) 'ThreatLabz 2025 Phishing Report: AI-Powered Threats & Zero Trust', [online] Available at: https://www.zscaler.com/learn/2025-phishing-report Accessed 24 Jan 2026.

Torkington, S. (2024) 'Resilience is key as emerging tech poses new cyber risks.', [online] World Economic Forum. Available at: https://www.weforum.org/stories/2024/10/cyber-resilience-emerging-technology-ai-cybersecurity/.

Tran, D.V., Nguyen, P.V., Le, L.P. and Thi, S. (2024) 'From awareness to behaviour: understanding cybersecurity compliance in Vietnam', *International journal of organizational analysis*, 33. doi:https://doi.org/10.1108/ijoa-12-2023-4147.

Tripathi, G., Ahad, M.A. and Casalino, G. (2023) 'A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges', *Decision Analytics Journal*, [online] 9, p.100344. doi:https://doi.org/10.1016/j.dajour.2023.100344.

Triplett, W.J. (2022) 'Addressing human factors in cybersecurity leadership', *Journal of Cybersecurity and Privacy*, 2, pp.478–497. doi:https://doi.org/10.3390/jcp2030026.

Tyagi, K., Nair, M., Niladhuri, S. and Abraham, A. (2020) 'Security, Privacy Research issues in Various Computing Platforms: A Survey and the Road Ahead', [online] Available at: https://ak-tyagi.com/static/pdf/6.pdf.

Uchendu, B., Mndzebele, N., Agaba, B. and Odongo, J. (2021) 'Developing a cyber security culture: Current practices and future needs', *arXiv*, 2106.14827. doi:https://doi.org/10.48550/arXiv.2106.14827.

Uddin, B. and Sharmin, A. (2020) '& 2) 13-23', *DUJASE*, [online] 5. Available at: https://arxiv.org/ftp/arxiv/papers/2105/2105.00192.pdf.

Union, E. (2021) 'Blockchain and distributed ledger technologies: Security and resilience', [online] Available at: https://www.enisa.europa.eu/publications/blockchain-and-dlt-security-and-resilience.

Upguard (2025) 'A Complete Guide to Data Breaches', [online] Available at: https://content.upguard.com/hubfs/resources/eBook%20-%20A%20Complete%20Guide%20to%20Data%20Breaches.pdf.

Vasudevan, S., Ramachandran, S. and Muthusamy, S. (2022) 'Non-technical factors in cyber resilience: Strategy, personnel, and communication', *Journal of Information Security and Applications*, 68, p.103233. doi:https://doi.org/10.1016/j.jisa.2022.103233.

Verizon (2023) '2023 Data Breach Investigations Report (DBIR)', [online] Available at: https://www.verizon.com/business/resources/Ta50/reports/2023-data-breach-investigations-report-dbir.pdf [Accessed Dec. 2023].

Villegas-Ch, W., Llanes-Cedeño, R. and Fuentes-Cedeño, M. (2023) 'A Framework for the Management of Security in a Smart University Based on Blockchain and IoT', *IEEE Access*, 11, pp.63784–63799. doi:https://doi.org/10.1109/ACCESS.2023.3288301.

W, L.E. and D, P.P. (2019) 'Cybersecurity policy framework and procedural compliance in public organisations'. pp.1–13.

Web, O. (2023) 'OWASP smart contract top 10 security risks', [online] Available at:

https://solidityscan.com/discover/owasp-smart-contract-top-10-security-risks-and-vulnerabilities-a-deep-dive-with-real-world-exploits-and-credshields-contribution/.

Whang, S.E., Roh, Y., Song, H. and Lee, J.-G. (2021) 'Data collection and quality challenges in deep learning: a data-centric AI perspective', *The VLDB Journal*, [online] 32, pp.791–813. doi:https://doi.org/10.1007/s00778-022-00775-9.

Winston (2026) 'Emerging Technology – Legal Glossary', [online] Available at: https://www.winston.com/en/legal-glossary/emerging-technology Viewed 24 Jan 2026.

Wood, G. (2014) 'Ethereum: A secure decentralised generalised transaction ledger'.

Working (2023) 'Security by Design for IoT Device Manufacturers TELECOMMUNICATION ENGINEERING CENTRE DEPARTMENT OF TELECOMMUNICATIONS MINISTRY OF COMMUNICATIONS GOVERNMENT OF INDIA RELEASE 2.0', [online] Available at: https://www.tec.gov.in/pdf/M2M/Security%20by%20Design%20for%20IoT%20Device%20Manufacturers.pdf [Accessed Jan. 2026].

World Economic Forum (2020) 'Personal data handling - WEF blockchain toolkit', [online] Available at: https://widgets.weforum.org/blockchain-toolkit/personal-data-handling/index.html.

www.fbi.gov. (n.d.) 'Common Scams & Crimes', [online] Available at: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes [Accessed Jan. 2023].

www.futuremarketinsights.com. (2023) 'Artificial Intelligence in Retail Market', [online] Available at: https://www.futuremarketinsights.com/reports/artificial-intelligence-in-retail-market.

YAACOB, MOHD NOORULFAKHRI, SYED and IDRIS, M. (2023) 'Managing Cybersecurity Risks in Emerging Technologies', *International Journal of Business and Technopreneurship (IJBT)*, 13, pp.253–270. doi:https://doi.org/10.58915/ijbt.v13i3.297.

Yaacob, I., Alzahrani, A., Alghamdi, R., Ahmed, N., Khalid, M. and Arshad, M. (2023) 'Blockchain-based security framework for industrial IoT networks: A systematic review', *IEEE Access*, 11, pp.45678–45701. doi:https://doi.org/10.1109/ACCESS.2023.3271234.

Yaga, D., Mell, P., Roby, N. and Scarfone, K. (2018) 'Blockchain Technology Overview', *ArXiv*, [online] abs/1906.11078. doi:https://doi.org/10.6028/nist.ir.8202.

Yamin, M.M., Ullah, M., Ullah, H. and Katt, B. (2021) 'Weaponized AI for cyber attacks', *Journal of information security and applications*. [online] doi:https://doi.org/10.1016/J.JISA.2020.102722.

Yin, H., Aryani, A., Petrie, S., Nambissan, A., Astudillo, A. and Cao, S. (2024) 'A Rapid Review of Clustering Algorithms', *ArXiv*, [online] abs/2401.07389. doi:https://doi.org/10.48550/arxiv.2401.07389.

Yinusa, A. and Faezipour, M. (2025) 'Evaluating Artificial Intelligence Robustness Against FGSM and PGD Adversarial Attacks with L-Norms Perturbations', [online] Springer. Available at: https://link.springer.com/chapter/10.1007/978-3-031-85628-0_23 Accessed 24 Jan 2026.

Yulianto, A. and Soewito, B. (2023) 'Robust security culture and resilience against ransomware', *Journal of Information Security and Applications*, 77, p.103218. doi:https://doi.org/10.1016/j.jisa.2023.103218.

Z, B.N., N, O.C., O, S.I. and Oni, O. (2025) 'The Integration of AI and blockchain technologies for secure data management in cybersecurity', *World Journal of Advanced Research and Reviews*, 25, pp.1666–1697.

Zand, M., Wu, X.B. and Morris, M.A. (2021) *Hands-On Smart Contract Development with Hyperledger Fabric V2*. Sebastopol, CA: 'O'Reilly Media, Inc.'

Zanke, A., Kossak, F., Binder, U. and Chasin, F. (2024) 'Assessing information security culture: A mixed-methods approach to navigating challenges in international corporate IT departments', *Computers & Security*, 143, p.103764. doi:https://doi.org/10.1016/j.cose.2023.103764.

Zhai, X., Chu, X., Chai, C.S., Morris, J., Istenic, A., Spector, M., Liu, J.-B., Yuan, J. and Li, Y. (2021) 'A Review of Artificial Intelligence (AI) in Education from 2010 to 2020', *Complexity*, [online] 2021, pp.1–18. doi:https://doi.org/10.1155/2021/8812542.

Zheng, J. and Namin, Akbar Siami (2019) 'A Survey on the Moving Target Defense Strategies:

An Architectural Perspective', *Journal of Computer Science and Technology*, 34, pp.207–233. doi:https://doi.org/10.1007/s11390-019-1906-z.

Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H. (2017) 'An overview of blockchain technology: Architecture, consensus, and future trends', pp.55–62.

Zhonghua, C. and B, G.S. (2022) 'Block chain Technology to Handle Security and Privacy for IoT Systems: Analytical Review', *International Journal of Electrical and Electronics Research*, 10, pp.74–79. doi:https://doi.org/10.37391/ijeer.100204.

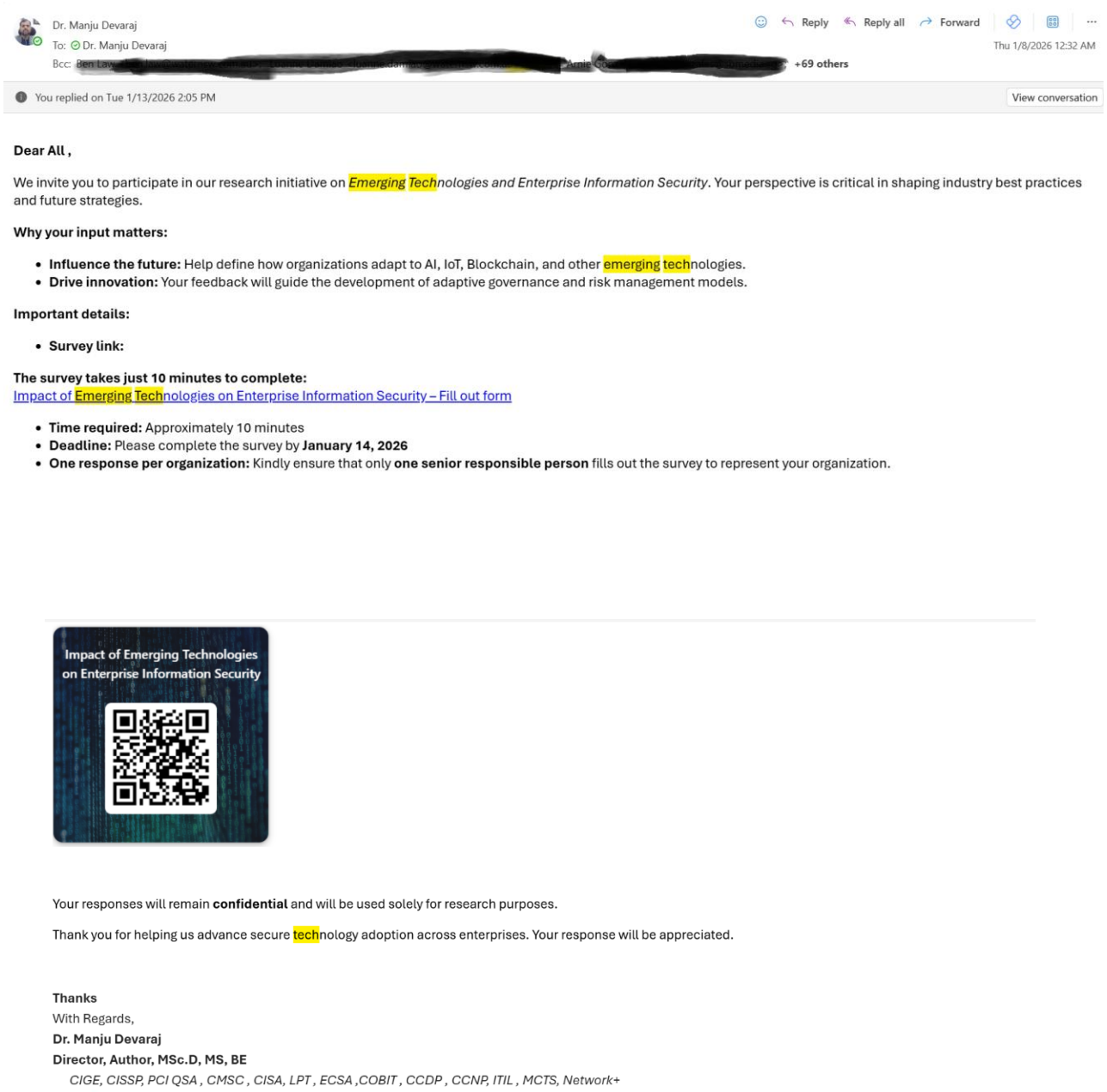
Zhu, Y. (2024) 'Cyber resilience: Integrating game, control, and learning theories', *IEEE Transactions on Information Forensics and Security*, 19, pp.1–16. doi:https://doi.org/10.1109/TIFS.2023.3338576.

Zubaydi, Haider D, Varga, P. and Molnár, S. (2023) 'Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review', *Sensors*, 23, p.788. doi:https://doi.org/10.3390/s23020788.

APPENDIX – A, B, C & D

Appendix A "Survey Instrument & Case Study Details."

A.1 SURVEY COVER LETTER



Dr. Manju Devaraj
To: Dr. Manju Devaraj
Bcc: [redacted] +69 others
Reply | Reply all | Forward
Thu 1/8/2026 12:32 AM

You replied on Tue 1/13/2026 2:05 PM — View conversation

Dear All ,

We invite you to participate in our research initiative on *Emerging Technologies and Enterprise Information Security*. Your perspective is critical in shaping industry best practices and future strategies.

Why your input matters:

- **Influence the future:** Help define how organizations adapt to AI, IoT, Blockchain, and other emerging technologies.
- **Drive innovation:** Your feedback will guide the development of adaptive governance and risk management models.

Important details:

- **Survey link:**

The survey takes just 10 minutes to complete:
Impact of Emerging Technologies on Enterprise Information Security – Fill out form

- **Time required:** Approximately 10 minutes
- **Deadline:** Please complete the survey by **January 14, 2026**
- **One response per organization:** Kindly ensure that only **one senior responsible person** fills out the survey to represent your organization.

Your responses will remain **confidential** and will be used solely for research purposes.

Thank you for helping us advance secure technology adoption across enterprises. Your response will be appreciated.

Thanks
With Regards,
Dr. Manju Devaraj
Director, Author, MSc.D, MS, BE
CIGE, CISSP, PCI QSA , CMSC , CISA, LPT , ECSA ,COBIT , CCDP , CCNP, ITIL , MCTS, Network+

A.3 INFORMED CONSENT FOR SURVEY

Title of the Study: Assessing the Impact of Emerging Technology on Enterprise Information Security

---

Researcher: Dr. Manju Devaraj

Program: Doctor of Business Administration (DBA)

Institution: Swiss School of Business and Management, Geneva

Supervisor: Dr. Ivica Katavic

Location of Study: Asia (Enterprise-level organizations)

Invitation to Participate

I am pleased to invite you to participate in an academic research study conducted as part of a Doctor of Business Administration (DBA) dissertation at the Swiss School of Business and Management in Geneva. Before deciding whether to participate, please read the information below carefully. Participation in this study is entirely voluntary.

Purpose of the Study

The purpose of this research is to examine how the adoption and integration of emerging technologies—specifically **Artificial Intelligence (AI), the Internet of Things (IoT), and Blockchain**—impact enterprise information security. The study also explores the role of cybersecurity leadership, organizational culture, and existing security frameworks in mitigating risks associated with these technologies.

The findings aim to contribute to academic knowledge and provide practical insights for enterprises, cybersecurity leaders, and policymakers on the adoption of secure and resilient technologies.

Nature of Participation

If you agree to participate, you will be asked to complete a **structured survey questionnaire** consisting of Likert-scale and multiple-choice questions related to:

- Adoption and integration of emerging technologies
- Information security risks, vulnerabilities, and incidents
- Cybersecurity frameworks, governance, and leadership practices

- Organizational readiness, resilience, and security culture

The survey is expected to take approximately **15–20 minutes** to complete.

Voluntary Participation and Right to Withdraw

Participation in this study is completely voluntary. You may decline to participate or withdraw from the study at any time without penalty, justification, or negative consequences. If you choose to withdraw, any data already submitted will be excluded from the analysis upon request, provided it has not yet been anonymized and aggregated.

Risks and Discomforts

This study involves **minimal risk**. No physical, psychological, legal, or professional harm is anticipated. You may skip any question you do not wish to answer. No sensitive personal data will be collected.

Benefits of Participation

While there may be no direct personal benefit, your participation will contribute to:

- Advancing research on emerging technologies and enterprise cybersecurity
- Improving understanding of leadership-driven cybersecurity resilience
- Supporting the development of adaptive and hybrid cybersecurity frameworks

---

Confidentiality and Anonymity

All information provided will be treated with strict confidentiality:

- No personally identifiable information (PII) will be collected
- Responses will be anonymized and reported only in aggregated form
- Individual participants or organizations will not be identifiable in the dissertation or any related publications

---

Data Protection and Storage

All research data will be handled in accordance with ethical research standards and information security best practices, including:

- Secure, password-protected storage of digital data

- Restricted access limited to the researcher
- Use of data solely for academic research purposes
- Compliance with applicable data protection principles .

Raw data will be retained only for the duration necessary to complete the research and analysis and will be securely deleted thereafter.

Use of Research Findings

The data collected may be used in:

- The doctoral dissertation
- Academic publications and conference presentations

In all cases, anonymity and confidentiality will be strictly maintained.

Questions or Concerns

If you have any questions about this study or your rights as a participant, you may contact: Dr. Manju Devaraj , Doctoral Researcher, Swiss School of Business and Management, Geneva

---

Consent Statement

By proceeding with the survey, you confirm that:

- You have read and understood the information provided above
- You voluntarily agree to participate in this research study
- You understand that you may withdraw at any time without consequence

---

Participant Consent (Tick/Confirm): ☐ I agree to participate in this study

Date: _____

A4. Survey Questionnaires

*Required

1. What is your name?

2. What is your email address? *

3. What is your age group? *

- ◯ Under 22
- ◯ 22-30
- ◯ 31-40
- ◯ 41-48
- ◯ 49-58
- ◯ 58 & above

4. What is your gender?

- ◯ Male
- ◯ Female
- ◯ Other
- ◯ Prefer not to say

5. What is your highest level of education?

- ◯ High School Diploma
- ◯ Bachelor's Degree
- ◯ Master's Degree
- ◯ Doctorate (Ph.D.)
- ◯ Other

6. What is your organization name?

7. What is your current employment status?

- ◯ Full-time
- ◯ Part-time
- ◯ Self-Employed
- ◯ Student
- ◯ Unemployed

8. Which sector do you primarily work in?

- ◯ Construction/Real Estate
- ◯ Finance/Banking
- ◯ Government/Policy
- ◯ Academia/Research
- ◯ Healthcare
- ◯ Retail
- ◯ Manufacturing
- ◯ Telecommunications
- ◯ Other

9. Total years of experience in your field?

- ◯ Less than 4 years
- ◯ 5 – 8 Years
- ◯ 9 – 13 Years
- ◯ 14 – 18 Years
- ◯ 19 – 22 Years
- ◯ 22+ years

10. What is your current role in the organization? *

- ◯ CIO
- ◯ IT Manager
- ◯ Cybersecurity Expert
- ◯ Other
- ◯ Head of Dept
- ◯ Director
- ◯ Sr. Consultant
- ◯ CISO
- ◯ CTO
- ◯ CEO
- ◯ Risk/Security/Compliance Manager
- ◯ Founder
- ◯ CA
- ◯ CFO
- ◯ Technology Specialist
- ◯ Business Development
- ◯ CIO

Researcher

General Manager

11. Which industry sector does your organization belong to? *

- ◯ Finance
- ◯ Healthcare
- ◯ Retail
- ◯ Manufacturing
- ◯ Telecommunications
- ◯ Service sector
- ◯ Engineering
- ◯ Supply chain
- ◯ Program Manager
- ◯ Other

12. How many employees does your organization have? *

- ◯ <100
- ◯ 100–500
- ◯ 501–1000
- ◯ >1000

13. What percentage of your IT budget is allocated to cybersecurity? *

- ◯ <10%
- ◯ 10–25%
- ◯ 26–50%
- ◯ >50%

14. Which emerging technologies has your organization adopted? (Select all that apply) *

- [ ] Artificial Intelligence (AI)
- [ ] Internet of Things (IoT)
- [ ] Blockchain
- [ ] None
- [ ] Other
- [ ] Quantum Computing
- [ ] Quantum Cryptography

15. How would you rate the level of integration of emerging technologies in your organization's operations? *

- ◯ Not integrated
- ◯ Low
- ◯ Medium
- ◯ High

16. How frequently does your organization conduct cybersecurity training and awareness programs? *

- ◯ Never
- ◯ Annually
- ◯ Quarterly
- ◯ Monthly

17. How effective do you believe these training programs are in improving employee security awareness? *

☆ ☆ ☆ ☆ ☆

Not effectiveHighly effective

18. What percentage of employees consistently comply with established security protocols? *

- ◯ <50%
- ◯ 50–75%
- ◯ 76–90%
- ◯ >90%

19. How quickly do employees respond to security alerts or incidents? *

- ◯ Immediately
- ◯ Within 24 hours
- ◯ Within a week Rarely/never
- ◯

⁞⁞⁞

20. How many cybersecurity incidents has your organization experienced in the past 12 months? *

- ◯ None
- ◯ 1–2
- ◯ 3–5
- ◯ >5

21. What was the most common type of incident?

- ◯ Data theft
- ◯ Service disruption
- ◯ Ransomware
- ◯ Other

22. Please rate the maturity of your organization for each of the following cybersecurity framework functions: *

	1 - Not mature	2	3	4	5 - Highly mature
Identify: Ability to recognize assets, threats, and vulnerabilities	◯	◯	◯	◯	◯
Protect: Implementation of safeguards	◯	◯	◯	◯	◯ and security controls
Detect: Ability to identify cybersecurity	◯	◯	◯	◯	◯ events promptly
Respond: Effectiveness in managing and	◯	◯	◯	◯	◯ mitigating incidents
Recover: Ability to restore operations after	◯	◯	◯	◯	◯ a security event

23. Which proactive security measures has your organization implemented? (Select all that apply) *

- ☐ Zero Trust Architecture
- ☐ Defense-in-Depth
- ☐ Moving Target Defense
- ☐ Security by Design
- ☐ Privacy by Design
- ☐ Security by Default

None

24. Please rate the effectiveness of each proactive security measure your organization has implemented:

	1 - Not effective	2	3	4	5 - Highly effective
Zero Trust					

Architecture	◯	◯	◯	◯	◯	
Defense-inDepth	◯	◯	◯	◯	◯	
Moving Target	◯	◯	◯	◯	◯	Defense
Security by Design	◯	◯	◯	◯	◯	
Privacy by Design	◯	◯	◯	◯	◯	
Security by Default	◯	◯	◯	◯	◯	

25. How involved is senior leadership in cybersecurity decision-making? *

Not involved ☆ ☆ ☆ ☆ ☆ Highly involved

26. Does your organization have a designated cybersecurity leader (e.g., CISO)? *

◯ Yes

◯ No

27. Please rate the following aspects of leadership commitment to cybersecurity in your organization: *

	1 - Not committed	2	3	4	5 - Highly committed
Leadership prioritizes	◯	◯	◯	◯	◯ cybersecurity
Resources allocated for	◯	◯	◯	◯	◯ cybersecurity
Regular review of cybersecurity	◯	◯	◯	◯	◯ policies
Support for employee training and	◯	◯	◯	◯	◯ awareness

28. How would you rate your organization's system availability over the past year? *

☆ ☆ ☆ ☆ ☆

Frequent downtimeHighly available

29. How confident are you in the assurance levels provided by your current cybersecurity controls? *

☆ ☆ ☆ ☆ ☆

Not confidentHighly confident

30. How resilient is your organization to cyber threats (ability to recover and adapt)? *

☆ ☆ ☆ ☆ ☆

Not resilientHighly resilient

31. How important is addressing the unique challenges of emerging technologies in your security frameworks? *

☆ ☆ ☆ ☆ ☆

Not importantExtremely important

32. How important is flexibility and adaptability in your security frameworks and strategies? *

☆ ☆ ☆ ☆ ☆

Not importantExtremely important

33. How important is interoperability between technologies and security solutions in your frameworks? *

☆ ☆ ☆ ☆ ☆

Not importantExtremely important

34. Is existing security frameworks (e.g., NIST, ISO) good enough to assess the impact of integrating novel or emerging technologies? *

☆ ☆ ☆ ☆ ☆

Not at all comfortableExtremely comfortable

35. Does your organization need an enhanced cybersecurity strategy or new frameworks to address emerging technology risks? *

Strongly disagree Strongly agree

A.5 – Individual Case Study Analysis

Case Study 1

How do varying levels of emerging technology integration affect the robustness of cybersecurity frameworks and strategies?

Independent Variable: Level of Integration of Emerging Technology(X2)

Dependent Variable: Robust Cybersecurity Framework, Cybersecurity Strategies – Resilience (Y3)

Case study report titled "Managing Cybersecurity Risks in Emerging Technologies" by Mohd Noorul fakhri Yaacob, Syed Zulkarnain Syed Idrus, and Mariam Idris, explores the impact of varying levels of emerging technology integration on the robustness of cybersecurity frameworks and strategies , explores the impact of varying levels of emerging technology integration on the robustness of cybersecurity frameworks and strategies. The analysis is based on the findings from the report "Managing Cybersecurity Risks in Emerging Technologies" by Mohd Noorulfakhri Yaacob, Syed Zulkarnain Syed Idrus, and Mariam Idris.

Levels of Technology Integration and Their Impact

Low Integration (10-25%)

Challenges: The limited integration of emerging technologies, such as AI, IoT, and blockchain, can lead to insufficient cybersecurity measures. Existing frameworks may not be fully equipped to handle the unique vulnerabilities introduced by these technologies.

Robustness: Cybersecurity frameworks may lack necessary updates and adaptations to address specific risks associated with emerging technologies, leading to potential gaps in protection.

Medium Integration (50%)

Challenges: Partial integration of emerging technologies requires a dynamic approach to cybersecurity. Organizations need to balance traditional security measures with new strategies tailored to the specific characteristics of the integrated technologies.

Robustness: Cybersecurity frameworks become more robust as they incorporate advanced security measures and protocols. However, managing both traditional and emerging technology risks can pose significant challenges.

High Integration (100%)

Challenges: Full integration of emerging technologies demands comprehensive, proactive and adaptive cybersecurity frameworks. The decentralized nature of technologies like blockchain and the extensive connectivity of IoT devices introduce new attack surfaces and vulnerabilities.

Robustness: Cybersecurity frameworks and strategies need to be highly robust, incorporating advanced security mechanisms such as zero trust, moving target defense(MTD), and defense-in-depth. Continuous monitoring, real-time threat intelligence, and proactive risk management are essential to maintain security.

Key Findings from the Case Study

Technical Challenges: Securing communication networks, protecting data and systems, and ensuring the reliability and integrity of emerging technologies are critical technical challenges. The complexity of these technologies requires advanced security measures and continuous updates to cybersecurity frameworks.

Organizational Challenges: Talent management, fostering a cybersecurity culture, and ensuring awareness among employees are significant organizational challenges. Effective training programs and a strong cybersecurity culture are essential to mitigate human errors and enhance the overall security posture.

Regulatory Challenges: Keeping up with evolving regulatory frameworks and compliance requirements is a major challenge. Organizations need to stay updated with regulatory changes and ensure their cybersecurity strategies align with legal obligations.

Further, Kumar, and Mallipeddi (2022) present several aspects of analysis related to different emerging technology aspects in their Case study report " Impact of Cybersecurity on Operations and Supply Chain Management: Emerging Trends and Future Research Directions."

Industry 4.0/5.0 and Cybersecurity Risks: The Analysis points out that adopting Industry 4.0 and 5.0 technologies (IoT, AI, cloud computing) increases cybersecurity risks. This supports H_o1, suggesting a potential correlation between high integration and increased risk initially. However, the article also calls for research into robust strategies to mitigate these risks, hinting at the possibility of achieving robust proactive frameworks and strategies(H_o4) even at high integration levels.

Blockchain Technology: The references to blockchain technology illustrate both the potential benefits (secure data sharing) and the challenges (inflated initial expectations leading to disappointment). This demonstrates the necessity of careful planning and investment in security infrastructure (relevant to H_o2 and H_o3). The positive impact on shareholder value when implemented successfully suggests that, with proper strategy, better integration can yield positive results (supporting H_o4).

Disruptive Technologies and Human-Machine Conflicts: Potential conflicts between humans and machines highlight the need for robust training and integration strategies(H_o4) to ensure security is not compromised during the adoption process. This strongly relates to H_o2, implying weaker security if proper training and integration are lacking (Kumar and Mallipeddi, 2022).

Study Outcome: Higher integration demands more countermeasures, higher investment & increased risks if not planned well; the issues can be addressed by implementing a proper Proactive Cybersecurity Framework that covers the lifecycle of activities and proactively preempts future issues.

Result & Conclusion:

According to a study by Mohd Noorulfakhri Yaacob, Syed Zulkarnain Syed Idrus, and Mariam Idris (2023), the level of emerging technology integration significantly impacts the robustness of cybersecurity frameworks and strategies. Higher levels of integration require more

comprehensive and adaptive cybersecurity measures to address the unique risks and vulnerabilities introduced by these technologies. Organizations must continuously evolve their cybersecurity frameworks to keep pace with technological advancements and emerging threats (Yaacob et al., 2023).

Overall, the case study analysis suggests a complex relationship between emerging technology integration and cybersecurity robustness. While high integration presents increased initial risks, it also offers the potential for highly robust cybersecurity through strategic implementation and investment. A balanced approach, with medium integration, might offer the most practical path, mitigate risks while leveraging the benefits of new technologies. Further research using quantitative data from real-world organizations is needed to solidify these findings.

Case Study 2

Does the implementation of cybersecurity training and awareness programs enhance employee compliance with security protocols?

Independent Variable: Cybersecurity Training and Awareness Programs

Dependent Variable: Employee Compliance with Security Protocols

Abrahams et al. (2024), in their study report "Cybersecurity Awareness and Education Programs: A Review of Employee Engagement and Accountability," highlights the critical role of employee engagement and accountability in the success of cybersecurity awareness programs. Their review emphasizes that effective programs extend beyond knowledge dissemination, incorporating interactive methodologies (workshops, simulated phishing exercises, online modules, gamified learning) to cultivate a culture of vigilance. The authors underscore the importance of a holistic approach, encompassing motivational factors, tailored learning experiences, and strong leadership support to foster a sense of responsibility and enhance engagement. Furthermore, the review stresses the necessity of accountability mechanisms, including robust monitoring systems, clear communication channels, and consequence management, to sustain the efficacy of security initiatives.

Several other studies indirectly support this assertion. Aşan (2024) explores the perception of cybersecurity among maritime industry employees, demonstrating varying levels of awareness across different roles. This suggests a need for tailored training programs to address

specific knowledge gaps and improve compliance. Similarly, Pankajakshan et al. (2024) demonstrate the significant impact of increased employee awareness on enhancing cybersecurity.

According to Dien Van Tran et al. (2024) , Maintaining robust cybersecurity requires not only technological safeguards but also a culture of security awareness among employees. This review assesses the efficacy of cybersecurity training and awareness programs in influencing employee behavior and adherence to security policies (Tran et al., 2025).

Several studies support a positive correlation between cybersecurity training and awareness programs and improved employee compliance.

Tran, D. V., Nguyen, P. V., Le, L. P., et al. (2024). FROM AWARENESS TO BEHAVIOUR: UNDERSTANDING CYBERSECURITY COMPLIANCE IN VIETNAM. *International Journal of Organizational Analysis*. This quantitative study in Vietnam demonstrated a strong positive association between security education, training, and awareness programs and employee cybersecurity awareness. Increased awareness positively influenced attitudes and intentions towards information security policy compliance (ISPC), ultimately leading to improved protective behaviors.

Tran, D. V., et al. (2023). EXPLORING THE INFLUENCE OF GOVERNMENT SOCIAL MEDIA ON CYBERSECURITY COMPLIANCE: EMPLOYEE ATTITUDES, MOTIVATION AND BEHAVIORS. *Journal of Asia Business Studies*. While not directly focused on training programs, this study highlights the positive impact of information dissemination and engagement on cybersecurity compliance attitudes, motivation, and protective behaviours. This suggests that effective communication strategies, often employed within training programs, can positively influence compliance.

Lee, C. S., et al. (2022). PATHWAYS TO CYBERSECURITY AWARENESS AND PROTECTION BEHAVIORS IN SOUTH KOREA. *Journal of Computer Information Systems*. This research revealed a positive association between cybersecurity awareness and cybersecurity behaviours. The study emphasizes the importance of raising awareness as a precursor to improved compliance, a key objective of training initiatives.

Kim, J., et al. (2021). HOPE, FEAR, AND CONSUMER BEHAVIORAL CHANGE AMID COVID-19: APPLICATION OF PROTECTION MOTIVATION THEORY. *International Journal of Consumer Studies*. And Wu, X., et al. (2021). EXPLORING INFLUENCE FACTORS OF WECHAT USERS' HEALTH INFORMATION SHARING

BEHAVIOR: BASED ON AN INTEGRATED MODEL OF TPB, UGT AND SCT. *International Journal of Human–Computer Interaction*. While not directly related to cybersecurity, these studies demonstrate the broader principle that targeted information campaigns can effectively modify behaviour. This principle is applicable to cybersecurity training, suggesting that well-designed programs can influence employees to adopt safer practices.

This case study provides compelling evidence suggesting that investing in cybersecurity training and awareness programs, alongside securing top management support, is crucial for improving employee compliance with security protocols. Future research should focus on replicating this study with larger samples and exploring contextual factors that might moderate these relationships. The cited supplementary research reinforces the importance of this finding within broader cybersecurity literature.

Several other studies corroborate the importance of training and awareness in improving cybersecurity behaviours:

Lee, C. S., et al. (2022). Pathways to cybersecurity awareness and protection behaviors in South Korea. *Journal of Computer Information Systems*. (This citation refers to a study suggesting a positive correlation between cybersecurity awareness and behaviors, supporting the Jamaican study's findings).

Donalds, C. M., et al. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *Int. J. Inf. Manag*. (This citation indicates other researchers have explored factors influencing cybersecurity compliance, lending further context).

In the case study by Okolo and Ighoroje (2024), they found significant positive correlations between several independent variables and the dependent variables. Specifically:

Compliance Adherence, Training Completion Rate, and Risk Awareness and Management significantly influenced Employee Feedback and Engagement. Higher levels of compliance adherence, training completion, and risk awareness were associated with increased positive employee feedback and engagement. (Okolo & Ighoroje, 2024).

Compliance Adherence, Security Policy Acknowledgements, and Training Completion Rate significantly impacted Incident Response Time. Improved adherence to security policies

and higher training completion rates correlated with faster incident response times. (Okolo & Ighoroje, 2024).

Compliance Adherence, Security Policy Acknowledgements, Training Completion Rate, and Risk Awareness and Management significantly contributed to Cybersecurity Culture. These factors collectively fostered a stronger cybersecurity culture within the banks (Okolo et al., 2024).

Study Outcome: Cybersecurity Training & Awareness(X5) , Positively impacts in enhancing cybersecurity

Result & Conclusion:

The reviewed case studies provide compelling evidence suggesting that investing in cybersecurity training and awareness programs, alongside securing top management support, is crucial for improving employee compliance with security protocols.

It also collectively indicates a strong positive relationship between cybersecurity training and awareness programs and employee compliance with security protocols. These programs' effectiveness appears to stem from their ability to raise awareness, shape attitudes, and influence intentions toward compliance, ultimately resulting in improved protective behaviors. Such Trainings & awareness activities should be part of a proactive Cybersecurity framework which is continuously evolving which supports $H_0$4 in this case as well .

Case Study 3

How does the investment in cybersecurity influence the organization's cybersecurity leadership and resilience?

Investment in comprehensive cybersecurity training and awareness programs appears to be a worthwhile strategy for improving organizational security posture by fostering a culture of security compliance among employees.

Independent Variable: Investment in Cybersecurity(X6)

Dependent Variable: Cybersecurity Leadership, Cyber Resilience(Y3)

According to research by Adedamola Oluokun, Ige and Nana (2024) & the report Building cyber resilience in fintech through AI and GRC integration: An exploratory Study.

Any Investments in cybersecurity significantly influence an organization's cybersecurity leadership and resilience. Strong financial commitment allows for acquiring and implementing

advanced technologies like Artificial Intelligence (AI) and robust Governance, Risk, and Compliance (GRC) frameworks. AI enhances threat detection and response capabilities, automating tasks and providing real-time insights into potential vulnerabilities. Simultaneously, comprehensive GRC frameworks ensure that cybersecurity strategies align with regulatory requirements and best practices, fostering a proactive risk management culture. This integrated approach not only strengthens an organization's defensive posture against common threats like phishing, malware, and ransomware but also equips it to address emerging sophisticated attacks leveraging AI and the Internet of Things (IoT). Consequently, improved cybersecurity leadership emerges through data-driven decision-making, continuous monitoring, and enhanced collaboration across teams. This proactive approach builds both technological and organizational resilience, enabling faster recovery and minimizing the impact of cyber incidents on operations, finances, and reputation. The resulting improved security posture enhances customer trust and strengthens the organization's competitive position" (Adedamola Oluokun et al., 2024).

Study Outcome: Investment in Cybersecurity would positively helps an organization to build Cyber resilience through building proactive cybersecurity framework which can include Adaptive Risk Management which is preemptive in nature .

Result & Conclusion:

Yes, investment in cybersecurity positively influences an organization's cybersecurity leadership which can help enterprise to build cybersecurity resilience by enabling the adoption of advanced technologies and robust proactive frameworks, fostering Adaptive risk management which can be proactive & preemptive in nature , this indeed supports $H_0 4$.

Case Study 4

Can regulatory compliance improve system availability and assurance levels in organizations when adopting emerging technologies?

Independent Variable: Existing Regulatory Compliance & Policies (X7)

Dependent Variable: System Availability, Assurance Levels (Resilience – Y3)

According to the study & analysis by Akash Takyar (2023) , a certain level of compliance might be necessary before significant improvements are observed, and beyond a certain point, further compliance efforts might yield diminishing returns. Furthermore, the specific impact of regulations varies depending on the industry, the specific emerging technologies involved, and the thoroughness of implementation.

Therefore, while regulatory compliance is a significant factor that can improve system availability and assurance levels, it's not a guaranteed solution, and its effectiveness depends on several contextual elements. The research supports the idea that compliance is a beneficial step, but it should be considered as part of a broader strategy for ensuring system reliability and security (Akash Takyar, 2023).

Artificial Intelligence in Retail: Use Cases, Challenges, and Future Trends

Artificial intelligence (AI) is rapidly transforming the retail landscape, impacting various aspects of business. AI-powered solutions are employed for personalized customer experiences through targeted recommendations and customized marketing campaigns; furthermore, AI streamlines operations through predictive analytics for inventory management and optimized supply chain logistics; finally, AI plays a crucial role in fraud detection and loss prevention, improving security and reducing financial losses. ("Artificial Intelligence in Retail Market," 2023)

Study Outcome: AI positively helped an organization to improve security & assurance levels in the organization.

Result & Conclusion:

AI's transformative potential in retail is undeniable, offering significant opportunities to enhance customer experience, streamline operations, and drive profitability. However, successful implementation requires careful consideration of the associated challenges, including high costs, data privacy concerns, and integration complexities, this in fact supports 'H₀3' that Leadership influences secure adoption which helps by reducing issues, secure adoption needs a good plan which calls for a Proactive framework which intern supports H₀4 & Cybersecurity Resilience . Addressing these challenges proactively and embracing future trends, such as advanced AI algorithms and explainable AI, will be crucial for retailers to fully capitalize on AI's transformative power and maintain a competitive edge in the evolving retail landscape.

Case Study 5

What effect does the type of emerging technology adopted have on the incidence and nature of security breaches?

Independent Variable: Type of Emerging Technology Implemented(X1)

Dependent Variable: Security Breaches & Incidences (Y2)

The Case study by Li and Liu (2021) , illustrates how the adoption of a specific emerging technology (AI) can influence the incidence and nature of security breaches. The text highlights

that AI can be used to improve cybersecurity by automating tasks, analyzing threats, and improving response times.

This suggests that the adoption of AI could potentially reduce the incidence of successful security breaches by proactively identifying and mitigating threats(Li and Liu, 2021).

Result & Conclusion:

While the number of publications on this topic is increasing, there's a need for more research focusing on the acquisition and representation of historical cybersecurity data to create practical AI-based solutions. The study produced a taxonomy classifying the reviewed articles based on cybersecurity functions, solution categories, and specific use cases of AI. It also analyzed the evolution of AI applications in cybersecurity, considering various functions, solution categories, use cases, and AI techniques employed. A key contribution is the integration of the existing literature and the identification of research gaps to guide future research in the field, specifically emphasizing the need for more robust historical data for effective AI-driven cybersecurity.

A Total of 5 case study reports were studied & analyzed. Further, a conclusion was drawn from each of the case studies reports analyzed.

Appendix B "Statistical Analysis "

Statistical Data– ANNOVA & Regression Analysis – RQ's & H_o1-H_o5

Table 5.5 Appendix B.1 - ANOVA for RQ 1

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1.766	4	.442	.831	.513[b]
	Residual	23.914	45	.531		
	Total	25.680	49			

2	Regression	7.329	7	1.047	2.396	.037[c]
	Residual	18.351	42	.437		
	Total	25.680	49			

a. Dependent Variable: How many cybersecurity incidents has your organisation experienced in the past 12 months?

b. Predictors: (Constant), Total years of experience in your field?, How would you rate the level of integration of emerging technologies in your organisation's operations?, How many employees does your organisation have?, What percentage of your IT budget is allocated to cybersecurity?

c. Predictors: (Constant), Total years of experience in your field?, How would you rate the level of integration of emerging technologies in your organization's operations?, How many employees does your organization have?, What percentage of your IT budget is allocated to cybersecurity?, Leadrship_index, Does your organization have a designated cybersecurity leader (e.g., CISO)?, How involved is senior leadership in cybersecurity decision-making?

Table 5.6

Appendix B.2 – Multiple Linear Regression Analysis for $H_0 1$

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.910	.692		1.315	.195

	How many employees does your organization have?	.043	.085	.079	.503	.617
	What percentage of your IT budget is allocated to cybersecurity?	.094	.216	.071	.435	.666
	How would you rate the level of integration of emerging technologies in your organisation's operations?	.126	.188	.099	.668	.508
	Total years of experience in your field?	.075	.074	.157	1.014	.316
2	(Constant)	3.106	.885		3.509	.001
	How many employees does your organisation have?	-.028	.091	-.053	-.314	.755
	What percentage of your IT budget is allocated to cybersecurity?	.198	.206	.150	.961	.342

	How would you rate the level of integration of emerging technologies in your organisation's operations?	.426	.214	.336	1.990	.053
	Total years of experience in your field?	.045	.068	.095	.666	.509
	Leadrship_index	.011	.110	.016	.101	.920
	How involved is senior leadership in cybersecurity decision-making?	-.718	.210	-.539	-3.414	.001
	Does your organisation have a designated cybersecurity leader (e.g., CISO)?	.156	.376	.065	.415	.680
a. Dependent Variable: How many cybersecurity incidents has your organisation experienced in the past 12 months?						

- The regression analysis indicates that the model is statistically significant ($F = 9.175$, $p < 0.001$), demonstrating that emerging technology adoption and integration level jointly predict cybersecurity incidents. The model explains 28.1% of the variance in incident frequency ($R^2 = 0.281$), with an adjusted R^2 of 0.250, suggesting moderate explanatory power given the sample size ($n = 50$).
- The level of integration of emerging technologies shows a positive and significant relationship with cybersecurity incidents ($\beta = 0.391$, $p = 0.007$). This suggests that higher levels of integration are associated with increased incident frequency, likely due to greater system complexity and expanded attack surfaces.

- Interestingly, the technology adoption variable demonstrates a significant negative relationship ($\beta = -0.571$, $p < 0.001$). This suggests that organizations formally adopting emerging technologies may implement structured controls that reduce incidents compared to partial or informal adoption. This indicates that integration intensity, rather than mere adoption, is the key risk factor.
- Overall, H_o1 is partially supported. While integration level increases incidents, structured technology adoption appears to mitigate risk when accompanied by governance mechanisms.

(H_o2): Integrating emerging technology into enterprise systems significantly correlates with increased specific vulnerabilities, such as data privacy issues and scalability concerns.

Variables Entered/Removed[a]

Model	Variables Entered	Variables Removed	Method
1	Vulnerability[b]	.	Enter

a. Dependent Variable: What was the most common type of incident?

b. All requested variables entered.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.353[a]	.125	.106	1.063

a. Predictors: (Constant), Vulnerability

Table 5.7

Appendix B.3: ANOVA for RQ 2

ANOVA[a]					
Model	Sum of Squares	df	Mean Square	F	Sig.

1	Regression	7.735	1	7.735	6.839	.012[b]
	Residual	54.285	48	1.131		
	Total	62.020	49			
a. Dependent Variable: What was the most common type of incident?						
b. Predictors: (Constant), Vulnerability						

Table 7. 1 Appendix

B.4: Simple Linear Regression Analysis for RQ 2

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	4.754	.740		6.427	.000
	Vulnerability	-.467	.178	-.353	-2.615	.012
a. Dependent Variable: What was the most common type of incident?						

- Integrating emerging technology into enterprise systems significantly correlates with increased specific vulnerabilities, such as data privacy issues and scalability concerns.

Construction of the Vulnerability Index

- To operationalize vulnerability associated with emerging technology integration, a composite Vulnerability Index was constructed. The index represents perceived exposure to risks arising from the integration of AI, IoT, Blockchain, and related technologies. Items reflecting vulnerability dimensions (e.g., privacy exposure, governance gaps, and implementation weaknesses) were aggregated into a single composite measure.
- Vulnerability_Index = Mean (Selected Vulnerability Indicators)
- This composite score provides a standardized measure of perceived enterprise vulnerability associated with technology integration.

Model Overview

- A linear regression analysis was conducted to examine the relationship between the Vulnerability Index (independent variable) and the most common type of cybersecurity incident experienced by organizations (dependent variable).
- The model was found to be statistically significant:
- $F(1,48) = 6.839$
- $p = 0.012$
- This indicates that vulnerability significantly predicts the variation in cybersecurity incident patterns.
- The model explains:
- $R^2 = 0.125$
- Adjusted $R^2 = 0.106$
- This suggests that approximately 12.5% of the variance in the type of cybersecurity incident is explained by the Vulnerability Index. Although the explanatory power is moderate, this is meaningful given the relatively small sample size (n = 50).

Interpretation of Coefficients

- The Vulnerability Index demonstrates a statistically significant relationship with cybersecurity incident type:
- Standardized Beta (β) = -0.353
- $t = -2.615$
- $p = 0.012$
- The significant coefficient confirms that perceived vulnerability associated with emerging technology integration meaningfully influences the type of cybersecurity incidents experienced by enterprises.
- The direction of the relationship (negative beta) depends on how incident categories were numerically coded in SPSS. However, the statistical significance confirms a systematic association between vulnerability exposure and cybersecurity outcomes.

Substantive Interpretation

- The findings suggest that enterprises reporting higher levels of integration-related vulnerabilities tend to experience distinct and measurable cybersecurity incident patterns. This supports the theoretical expectation that emerging technology integration expands

the attack surface, introduces data governance complexities, and increases exposure to privacy and scalability risks.

- While the effect size ($R^2 = 0.125$) indicates a moderate explanatory contribution, the statistically significant association reinforces the argument that vulnerability management is a critical determinant of cybersecurity outcomes in digitally transforming enterprises.

Hypothesis (H_o3): Strong information security leadership positively influences the secure adoption and implementation of Emerging technologies, reducing the likelihood of security breaches.

Table 5.8

H_o3 Hypothesis Testing – Information security leadership vs Adoption

Variables Entered/Removed[a]

Model	Variables Entered	Variables Removed	Method
1	Leadrship_index, How would you rate the level of integration of emerging technologies in your organization's operations?[b]	.	Enter
2	ET_Leadership[b]	.	Enter

a. Dependent Variable: How resilient is your organization to cyber threats (ability to recover and adapt)?

b. All requested variables entered.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.465[a]	.217	.183	.635

2	.482[b]	.232	.182	.635

a. Predictors: (Constant), Leadrship_index, How would you rate the level of integration of emerging technologies in your organization's operations?

b. Predictors: (Constant), Leadrship_index, How would you rate the level of integration of emerging technologies in your organization's operations?, ET_Leadership

Table 5.9

Appendix B.5: ANOVA for RQ 3

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	5.240	2	2.620	6.501	.003[b]
	Residual	18.940	47	.403		
	Total	24.180	49			
2	Regression	5.619	3	1.873	4.641	.006[c]
	Residual	18.561	46	.404		
	Total	24.180	49			

a. Dependent Variable: How resilient is your organization to cyber threats (ability to recover and adapt)?

b. Predictors: (Constant), Leadrship_index, How would you rate the level of integration of emerging technologies in your organization's operations?

c. Predictors: (Constant), Leadrship_index, How would you rate the level of integration of emerging technologies in your organization's operations?, ET_Leadership

Table 5.10

Appendix B.6: Moderated Regression(Interactive test) Analysis for RQ 3

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.671	.576		4.634	.000
	How would you rate the level of integration of emerging technologies in your organization's operations?	.186	.163	.151	1.139	.261
	Leadrship_index	.273	.089	.407	3.071	.004
2	(Constant)	-4.733	7.661		-.618	.540
	How would you rate the level of integration of emerging technologies in your organization's operations?	2.663	2.561	2.166	1.040	.304
	Leadrship_index	1.818	1.597	2.711	1.139	.261
	ET_Leadership	-.516	.533	-3.391	-.969	.338

a. Dependent Variable: How resilient is your organization to cyber threats (ability to recover and adapt)?

Model 1: Main Effects Only

- Model 1 includes:
- Integration (Q15)
- Leadership_Index
- The model is statistically significant:
- $F(2,47) = 6.501$, $p = 0.003$
- $R^2 = 0.217$
- Adjusted $R^2 = 0.183$

- This means integration and leadership together explain 21.7% of the variance in organizational resilience.
- Looking at coefficients:
- Leadership_Index ($\beta = 0.407$, $p = 0.004$) → Significant and positive
- Integration ($\beta = 0.151$, $p = 0.261$) → Not significant
- This indicates that leadership significantly improves resilience, while integration alone does not significantly predict resilience.

Model 2: Adding Interaction (Moderation Test)

- Model 2 adds the interaction term (ET_Leadership).
- The model remains significant:
- $F(3,46) = 4.641$, $p = 0.006$
- $R^2 = 0.232$
- Adjusted $R^2 = 0.182$
- However, The increase in R^2 from Model 1 to Model 2 is very small:
- $0.217 \rightarrow 0.232$
- (Only 1.5% additional variance explained)

Interaction Effect

- The interaction term:
- $\beta = -3.391$
- $p = 0.338$
- The interaction is not statistically significant.
- Therefore:
- Leadership does NOT significantly moderate the relationship between integration and resilience.

Interpretation of $H_0 3$

- The results show that leadership has a strong and direct positive effect on resilience. Organizations with stronger cybersecurity leadership demonstrate higher resilience.
- However, leadership does not significantly change the relationship between emerging technology integration and resilience. The non-significant interaction term indicates that

leadership does not weaken or strengthen the impact of technology integration on security posture.

Hypothesis($H_0$4): A Proactive cybersecurity framework may combine risk-driven strategy, strong culture and governance, and advanced technical controls with resilience and user-centric design to withstand & recover from evolving threats.

Table 5.11

Appendix B.7: ANNOVA & Hierarchical M. Regression Analysis for RQ 4

Variables Entered/Removed[a]

Model	Variables Entered	Variables Removed	Method
1	Leadrship_index, How would you rate the level of integration of emerging technologies in your organization's operations?[b]	.	Enter

a. Dependent Variable: How resilient is your organization to cyber threats (ability to recover and adapt)?

b. All requested variables entered.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.465[a]	.217	.183	.635

a. Predictors: (Constant), Leadrship_index, How would you rate the level of integration of emerging technologies in your organization's operations?

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	5.240	2	2.620	6.501	.003[b]
	Residual	18.940	47	.403		
	Total	24.180	49			

a. Dependent Variable: How resilient is your organization to cyber threats (ability to recover and adapt)?

b. Predictors: (Constant), Leadrship_index, How would you rate the level of integration of emerging technologies in your organization's operations?

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.671	.576		4.634	.000
	How would you rate the level of integration of emerging technologies in your organization's operations?	.186	.163	.151	1.139	.261
	Leadrship_index	.273	.089	.407	3.071	.004

a. Dependent Variable: How resilient is your organization to cyber threats (ability to recover and adapt)?

Variables Entered/Removed[a]

Model	Variables Entered	Variables Removed	Method

1	Leadrship_index, How would you rate the level of integration of emerging technologies in your organization's operations?[b]	.	Enter

a. Dependent Variable: Proactive_Framework

b. All requested variables entered.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.707[a]	.500	.479	.53233

a. Predictors: (Constant), Leadrship_index, How would you rate the level of integration of emerging technologies in your organization's operations?

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	13.345	2	6.672	23.546	.000[b]
	Residual	13.319	47	.283		
	Total	26.663	49			

a. Dependent Variable: Proactive_Framework

b. Predictors: (Constant), Leadrship_index, How would you rate the level of integration of emerging technologies in your organization's operations?

Coefficients[a]

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		

	(Constant)	2.777	.483		5.748	.000
1	How would you rate the level of integration of emerging technologies in your organization's operations?	-.337	.137	-.261	-2.468	.017
	Leadrship_index	.507	.075	.720	6.798	.000

a. Dependent Variable: Proactive_Framework

Variables Entered/Removed[a]

Model	Variables Entered	Variables Removed	Method
1	Leadrship_index, How would you rate the level of integration of emerging technologies in your organization's operations?[b]	.	Enter
2	Proactive_Framework[b]	.	Enter

a. Dependent Variable: How resilient is your organization to cyber threats (ability to recover and adapt)?

b. All requested variables entered.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.465[a]	.217	.183	.635
2	.597[b]	.356	.314	.582

a. Predictors: (Constant), Leadrship_index, How would you rate the level of integration of emerging technologies in your organization's operations?

b. Predictors: (Constant), Leadrship_index, How would you rate the level of integration of emerging technologies in your organization's operations?, Proactive_Framework

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	5.240	2	2.620	6.501	.003[b]
	Residual	18.940	47	.403		
	Total	24.180	49			
2	Regression	8.614	3	2.871	8.485	.000[c]
	Residual	15.566	46	.338		
	Total	24.180	49			

a. Dependent Variable: How resilient is your organization to cyber threats (ability to recover and adapt)?

b. Predictors: (Constant), Leadrship_index, How would you rate the level of integration of emerging technologies in your organization's operations?

c. Predictors: (Constant), Leadrship_index, How would you rate the level of integration of emerging technologies in your organization's operations?, Proactive_Framework

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.671	.576		4.634	.000
	How would you rate the level of integration of emerging technologies in your organization's operations?	.186	.163	.151	1.139	.261
	Leadrship_index	.273	.089	.407	3.071	.004

2	(Constant)	1.273	.689		1.847	.071
	How would you rate the level of integration of emerging technologies in your organization's operations?	.355	.159	.289	2.239	.030
	Leadrship_index	.018	.115	.027	.156	.877
	Proactive_Framework	.503	.159	.529	3.158	.003

a. Dependent Variable: How resilient is your organization to cyber threats (ability to recover and adapt)?

- In this analysis, organizational resilience (Q30) was the dependent variable, while Proactive_Framework served as the key explanatory construct. Leadership and integration level were included as predictors to examine both direct and indirect effects.

Model 1: Leadership and Integration Predicting Resilience

- The first regression model examined whether leadership and emerging technology integration predict organizational resilience. The model was statistically significant ($F(2,47) = 6.501$, $p = 0.003$), explaining 21.7% of the variance in resilience ($R^2 = 0.217$; Adjusted $R^2 = 0.183$).
- Leadership was a significant positive predictor of resilience ($\beta = 0.407$, $p = 0.004$), indicating that stronger cybersecurity leadership enhances an organization's ability to recover and adapt to cyber threats. However, the level of emerging technology integration was not statistically significant ($\beta = 0.151$, $p = 0.261$), suggesting that integration alone does not directly determine resilience.
- This indicates that governance and leadership structures are more influential than technological integration in shaping resilience capacity.

Model 2: Predicting Proactive Framework Strength

- The second regression assessed whether leadership and integration predict the strength of the proactive cybersecurity framework. The model was highly significant ($F(2,47) =$

23.546, $p < 0.001$), explaining 50% of the variance in Proactive_Framework ($R^2 = 0.500$; Adjusted $R^2 = 0.479$).

- Leadership demonstrated a very strong positive effect on proactive framework strength ($\beta = 0.720$, $p < 0.001$). This indicates that organizations with stronger cybersecurity leadership are substantially more likely to develop robust governance-driven and strategically aligned security frameworks.
- Interestingly, integration level showed a significant negative relationship ($\beta = -0.261$, $p = 0.017$), suggesting that higher levels of integration may strain or challenge framework robustness unless adequately supported by leadership and governance mechanisms.

Model 3: Adding Proactive Framework to Predict Resilience

- In the third regression model, Proactive_Framework was added to predict resilience alongside leadership and integration. The model became stronger and highly significant ($F(3,46) = 8.485$, $p < 0.001$), explaining 35.6% of the variance in resilience ($R^2 = 0.356$; Adjusted $R^2 = 0.314$). This represents a substantial improvement over Model 1.
- Most importantly: Proactive_Framework was a strong and significant predictor of resilience ($\beta = 0.529$, $p = 0.003$).
- Leadership became non-significant ($\beta = 0.027$, $p = 0.877$).
- Integration became significant ($\beta = 0.289$, $p = 0.030$).
- The loss of significance for leadership after adding Proactive_Framework indicates that the effect of leadership on resilience operates primarily through strengthening the proactive cybersecurity framework.

Overall Interpretation of H_o4

- The findings provide strong empirical support for H_o4. While leadership initially appears to enhance resilience directly, its effect becomes indirect once proactive framework robustness is introduced into the model. This suggests that leadership contributes to resilience by building structured, governance-driven cybersecurity frameworks rather than influencing resilience independently.
- The significant effect of Proactive_Framework ($\beta = 0.529$) indicates that framework robustness is the strongest predictor of resilience in the model. Organizations with risk-

driven strategy, strong governance alignment, and adaptive security architecture demonstrate significantly higher resilience against cyber threats.

- Furthermore, the increase in R^2 from 0.217 to 0.356 after adding the proactive framework highlights its critical explanatory role in determining organizational resilience.

Hypothesis ($H_0$5): Implementing comprehensive security policies & frameworks and adhering to industry best practices significantly reduces the security risks associated with AI, IoT, and Blockchain integration.

Variables Entered/Removed[a]

Model	Variables Entered	Variables Removed	Method
1	How would you rate the level of integration of emerging technologies in your organization's operations?[b]	.	Enter

a. Dependent Variable: How many cybersecurity incidents has your organization experienced in the past 12 months?

b. All requested variables entered.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.138[a]	.019	-.001	.724

a. Predictors: (Constant), How would you rate the level of integration of emerging technologies in your organization's operations?

Table 5.12

Appendix B.8: ANNOVA for RQ 5

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.490	1	.490	.934	.339[b]
	Residual	25.190	48	.525		
	Total	25.680	49			

a. Dependent Variable: How many cybersecurity incidents has your organization experienced in the past 12 months?

b. Predictors: (Constant), How would you rate the level of integration of emerging technologies in your organization's operations?

Table 5.13

Appendix B.9: Simple linear Regression for RQ 5

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.360	.589		2.311	.025
	How would you rate the level of integration of emerging technologies in your organization's operations?	.175	.181	.138	.966	.339

a. Dependent Variable: How many cybersecurity incidents has your organization experienced in the past 12 months?

Direct Effect of Integration on Cybersecurity Incidents

- The regression model was not statistically significant:
- $F(1,48) = 0.934$
- $p = 0.339$
- $R^2 = 0.019$
- Adjusted $R^2 = -0.001$
- The model explains only 1.9% of the variance in cybersecurity incidents, indicating extremely weak explanatory power.
- The integration variable showed:
- $\beta = 0.138$
- $p = 0.339$
- This indicates that the level of emerging technology integration does not significantly predict the number of cybersecurity incidents experienced by organizations.

Interpretation of the Direct Relationship

- The non-significant result suggests that, within this sample, higher levels of integration of AI, IoT, and Blockchain technologies are not associated with increased or decreased cybersecurity incidents. This indicates that technology adoption alone does not inherently determine breach frequency.
- The weak relationship may be influenced by several factors:
- Limited variability in incident data (majority reported 1–2 incidents)
- Small sample size (n = 50)
- Incidents being episodic events rather than structural security posture indicators

Why Mediation Was Not Further Processed

- For mediation analysis (Baron & Kenny framework), the first requirement is:
- The independent variable must significantly predict the dependent variable.
- Integration (Q15) → Cybersecurity Incidents (Q20)
- was not statistically significant.
- Because the total effect (IV → DV) was not established, classical mediation conditions were not satisfied. Without a significant relationship between integration and incidents, there is no effect for policy framework strength to mediate.

- Therefore, proceeding with mediation analysis would not be statistically appropriate or theoretically justified under the Baron & Kenny approach.
- H_o5 is not supported when cybersecurity incidents are used as the outcome variable. Integration level does not significantly predict breach frequency, and therefore mediation through policy framework strength was not further tested.
- These results suggest that comprehensive security policies and governance frameworks may influence broader security posture (e.g., resilience) rather than directly reducing reported incident frequency.

Model Comparison – Overall Model test

Overall Model:

Table 5.14

Appendix B.10: Overall Model ANNOVA & Multiple Regression

Variables Entered/Removed[a]

Model	Variables Entered	Variables Removed	Method
1	ET_Leadership, Policy_Framework_Strength, How would you rate the level of integration of emerging technologies in your organization's operations?, Proactive_Framework, Leadrship_index[b]	.	Enter

a. Dependent Variable: How resilient is your organization to cyber threats (ability to recover and adapt)?

b. All requested variables entered.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.719[a]	.516	.461	.515

a. Predictors: (Constant), ET_Leadership, Policy_Framework_Strength, How would you rate the level of integration of emerging technologies in your organization's operations?, Proactive_Framework, Leadrship_index

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	12.487	5	2.497	9.398	.000[b]
	Residual	11.693	44	.266		
	Total	24.180	49			

a. Dependent Variable: How resilient is your organization to cyber threats (ability to recover and adapt)?

b. Predictors: (Constant), ET_Leadership, Policy_Framework_Strength, How would you rate the level of integration of emerging technologies in your organization's operations?, Proactive_Framework, Leadrship_index

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	7.986	6.713		1.190	.241
	How would you rate the level of integration of emerging technologies in your organization's operations?	-2.172	2.290	-1.767	-.948	.348

	Leadrship_index	-1.627	1.472	-2.426	-1.106	.275
	Proactive_Framework	2.239	.478	2.351	4.683	.000
	Policy_Framework_Strength	-1.435	.376	-1.711	-3.817	.000
	ET_Leadership	.494	.478	3.248	1.034	.307

a. Dependent Variable: How resilient is your organization to cyber threats (ability to recover and adapt)?

Model Fit and Predictive Power

- The overall regression model was statistically significant:
- $F(5,44) = 9.398$
- $p < 0.001$
- The model explains 51.6% of the variance in organizational resilience ($R^2 = 0.516$; Adjusted $R^2 = 0.461$). This indicates strong predictive capability, particularly given the modest sample size (n = 50). The adjusted R^2 of 0.461 suggests that nearly half of the variability in resilience can be explained by the integrated set of governance, leadership, and framework-related factors.
- This demonstrates that the overall structural model has substantial explanatory power in understanding enterprise security posture.

Effects of Emerging Technology Integration

- The level of emerging technology integration was not a significant predictor of resilience in the final model ($\beta = -1.767$, $p = 0.348$). This suggests that integration intensity alone does not determine organizational resilience when governance and framework factors are considered simultaneously.
- This finding reinforces earlier results indicating that technology adoption itself is not inherently associated with stronger or weaker security posture.

Effects of Leadership

- Leadership_Index was not statistically significant in the presence of other predictors ($\beta = -2.426$, $p = 0.275$). This suggests that leadership does not directly influence resilience once proactive and policy framework variables are accounted for.
- This result indicates that leadership effects may operate indirectly through the development of structured frameworks rather than influencing resilience independently.

- The interaction term (ET_Leadership) was also not significant ($\beta = 3.248$, $p = 0.307$), indicating that leadership does not significantly moderate the relationship between integration and resilience in the full model.

Effects of Proactive Framework

- Proactive_Framework emerged as a strong and highly significant predictor of resilience: $p < 0.001$
- This indicates that organizations with stronger proactive cybersecurity frameworks demonstrate significantly higher resilience against cyber threats. The magnitude and statistical strength of this predictor suggest that governance-driven and strategically aligned frameworks are central determinants of organizational adaptability and recovery capacity.
- Among all variables in the model, Proactive_Framework is the most influential predictor of resilience.

Effects of Policy Framework Strength

- Policy_Framework_Strength was also statistically significant:
- $p < 0.001$
- Interestingly, the coefficient is negative. This may indicate that organizations with more formalized policies report lower resilience perceptions, possibly reflecting stricter internal assessments, higher compliance sensitivity, or reactive strengthening of policies following prior security challenges.
- This result suggests that policy strength plays a significant role in shaping resilience perceptions, although the direction may reflect complex governance dynamics rather than a simple protective effect.

Proof of SPSS – Stat Viewer screen

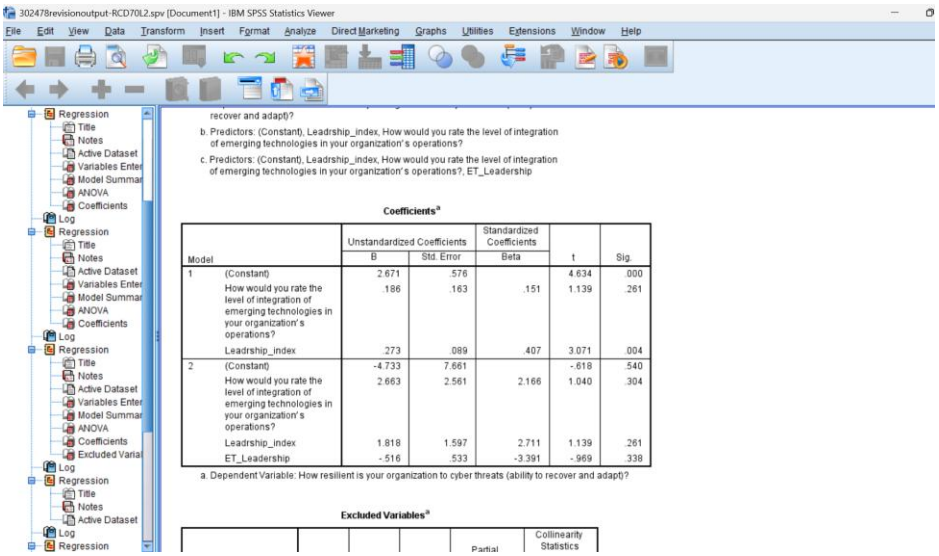


Figure 5.9

SPSS Screen with Data view

Appendix C “NIST AI & ETSI IoT Framework Controls “

NIST AI RMF Controls

Table 5.15

NIST AI RMF 2.0 Framework Control , Data Source : (NIST, 2024)

NIST AI RMF - Controls Checklist - GOVERN , MAP , ME		
Function	**Control**	**Description**
Govern	1.1	Legal and regulatory requirements involving AI are understood, managed, and documented.
	1.2	Characteristics of trustworthy AI are integrated into organizational policies, processes, and procedures.
	1.3	Processes and procedures are in place to determine the needed level of risk management activities based on the organization's risk tolerance.
	1.4	Risk management process and its outcomes are established through transparent policies, procedures, and other controls based on organizational risk priorities.
	1.5	Ongoing monitoring and periodic review of the risk management process and its outcomes are planned, organizational roles and responsibilities are clearly defined.
	1.6	Mechanisms are in place to inventory AI systems and are resourced according to organizational risk priorities.
	1.7	Processes and procedures are in place for decommissioning and phasing out of AI systems safely and in a manner that does not increase risks or decrease the organization’s trustworthiness.
	2.1	Roles and responsibilities and lines of communication related to mapping, measuring, and managing AI risks are documented and are clear to individuals and teams throughout the organization.
	2.2	The organization’s personnel and partners receive AI risk management training to enable them to perform their duties and responsibilities consistent with related policies, procedures, and agreements.
	2.3	Executive leadership of the organization takes responsibility for decisions about risks associated with AI system development and deployment.
	3.1	Decision-makings related to mapping, measuring, and managing AI risks throughout the lifecycle is informed by a diverse team.
	3.2	Policies and procedures are in place to define and differentiate roles and responsibilities for human-AI configurations and oversight of AI systems.
	4.1	Organizational policies, and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of AI systems to minimize negative impacts.
	4.2	Organizational teams document the risks and potential impacts of the AI technology they design, develop, deploy, evaluate and use, and communicate about the impacts more broadly.
	4.3	Organizational practices are in place to enable AI testing, identification of incidents, and information sharing.
	5.1	Organizational policies and practices are in place to collect, consider, prioritize, and integrate feedback from those external to the team that developed or deployed the AI system regarding the potential individual and societal impacts related to AI risks.
	5.2	Mechanisms are established to enable AI actors to regularly incorporate adjudicated feedback from relevant AI actors into system design and implementation.
	6.1	Policies and procedures are in place that address AI risks associated with third-party entities, including risks of infringement of a third party’s intellectual property or other rights.
	6.2	Contingency processes are in place to handle failures or incidents in third-party data or AI systems deemed to be high-risk.
	1.1	A determination is made as to whether the AI system achieves its intended purpose and stated objectives and whether its development or deployment should proceed.
	1.2	Treatment of documented AI risks is prioritized based on impact, likelihood, or available resources or methods.
	1.3	Responses to the AI risks deemed high priority as identified by the Map function, are developed, planned, and documented.
	1.4	Negative residual risks to both downstream acquirers of AI systems and end users are documented.
	2.1	Resources required to manage AI risks are taken into account, along with viable non-AI alternative systems, approaches, or methods – to reduce the magnitude or likelihood of potential impacts.
	2.2	Mechanisms are in place and applied to sustain the value of deployed AI systems.
	2.3	Procedures are followed to respond to and recover from a previously unknown risk when it is identified.
	2.4	Mechanisms are in place and applied, responsibilities are assigned and understood to supersede, disengage, or deactivate AI systems that demonstrate performance or outcomes inconsistent with intended use.
	3.1	AI risks and benefits from third-party resources are regularly monitored, and risk controls are applied and documented.
	3.2	Pre-trained models which are used for development are monitored as part of AI system regular monitoring and maintenance.
	4.1	Post-deployment AI system monitoring plans are implemented, including mechanisms for capturing and evaluating input from users and other relevant AI actors, appeal and override, decommissioning, incident response, recovery, and change management.
	4.2	Measurable activities for continual improvements are integrated into AI system updates and include regular engagement with interested parties, including relevant AI actors.
	4.3	Incidents and errors are communicated to relevant AI actors including affected communities. Processes for tracking, responding to, and recovering from incidents and errors are followed and documented.

Map	1.1	Intended purpose, potentially beneficial uses, context-specific laws, norms and expectations, and prospective settings in which the AI system will be deployed are understood and documented.
	1.2	Inter-disciplinary AI actors, competencies, skills and capacities for establishing context reflect demographic diversity and broad domain and user experience expertise, and their participation is documented. Opportunities for interdisciplinary collaboration are prioritized.
	1.3	The organization's mission and relevant goals for the AI technology are understood and documented.
	1.4	The business value or context of business use has been clearly defined or – in the case of assessing existing AI systems – re-evaluated.
	1.5	Organizational risk tolerances are determined and documented.
	1.6	System requirements are elicited from and understood by relevant AI actors. Design decisions take socio-technical implications into account to address AI risks.
	2.1	The specific task, and methods used to implement the task, that the AI system will support is defined.
	2.2	Information about the AI system's knowledge limits and how system output may be utilized and overseen by humans is documented. Documentation provides sufficient information to assist relevant AI actors when making informed decisions and taking subsequent actions.
	2.3	Scientific integrity and TEVV considerations are identified and documented, including those related to experimental design, data collection and selection, system trustworthiness, and construct validation.
	3.1	Potential benefits of intended AI system functionality and performance are examined and documented.
	3.2	Potential costs, including non-monetary costs, which result from expected or realized AI errors or system functionality and trustworthiness - as connected to organizational risk tolerance - are examined and documented.
	3.3	Targeted application scope is specified and documented based on the system's capability, established context, and AI system categorization.
	3.4	Processes for operator and practitioner proficiency with AI system performance and trustworthiness – and relevant technical standards and certifications – are defined, assessed and documented.
	3.5	Processes for human oversight are defined, assessed, and documented in accordance with organizational policies from GOVERN function.
	4.1	Approaches for mapping AI technology and legal risks of its components – including the use of third-party data or software – are in place, followed, and documented, as are risks of infringement of a third-party's intellectual property or other rights.
	4.2	Internal risk controls for components of the AI system including third-party AI technologies are identified and documented.
	5.1	Likelihood and magnitude of each identified impact (both potentially beneficial and harmful) based on expected use, past uses of AI systems in similar contexts, public incident reports, feedback from those external to the team that developed or deployed the AI system, or other data are identified and documented.
	5.2	Practices and personnel for supporting regular engagement with relevant AI actors and integrating feedback about positive, negative, and unanticipated impacts are in place and documented.
Manage	1.1	Approaches and metrics for measurement of AI risks enumerated during the Map function are selected for implementation starting with the most significant AI risks. The risks or trustworthiness characteristics that will not – or cannot – be measured are properly documented.
	1.2	Appropriateness of AI metrics and effectiveness of existing controls is regularly assessed and updated including reports of errors and impacts on affected communities.
	1.3	Internal experts who did not serve as front-line developers for the system and/or independent assessors are involved in regular assessments and updates. Domain experts, users, AI actors external to the team that developed or deployed the AI system, and affected communities are consulted in support of assessments as necessary per organizational risk tolerance.
	2.1	Test sets, metrics, and details about the tools used during test, evaluation, validation, and verification (TEVV) are documented.
	2.2	Evaluations involving human subjects meet applicable requirements (including human subject protection) and are representative of the relevant population.
	2.3	AI system performance or assurance criteria are measured qualitatively or quantitatively and demonstrated for conditions similar to deployment setting(s). Measures are documented.
	2.4	The functionality and behavior of the AI system and its components – as identified in the MAP function – are monitored when in production.
	2.5	The AI system to be deployed is demonstrated to be valid and reliable. Limitations of the generalizability beyond the conditions under which the technology was developed are documented.
	2.6	AI system is evaluated regularly for safety risks – as identified in the MAP function. The AI system to be deployed is demonstrated to be safe, its residual negative risk does not exceed the risk tolerance, and can fail safely, particularly if made to operate beyond its knowledge limits. Safety metrics implicate system reliability and robustness, real-time monitoring, and response times for AI system failures.
	2.7	AI system security and resilience – as identified in the MAP function – are evaluated and documented.
	2.8	Risks associated with transparency and accountability – as identified in the MAP function – are examined and documented.
	2.9	The AI model is explained, validated, and documented, and AI system output is interpreted within its context – as identified in the MAP function – and to inform responsible use and governance.
	2.1	Privacy risk of the AI system – as identified in the MAP function – is examined and documented.
	2.11	Fairness and bias – as identified in the MAP function – is evaluated and results are documented.
	2.12	Environmental impact and sustainability of AI model training and management activities – as identified in the MAP function – are assessed and documented.
	2.13	Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented.
	3.1	Approaches, personnel, and documentation are in place to regularly identify and track existing, unanticipated, and emergent AI risks based on factors such as intended and actual performance in deployed contexts.
	3.2	Risk tracking approaches are considered for settings where AI risks are difficult to assess using currently available measurement techniques or where metrics are not yet available.
	3.3	Feedback processes for end users and impacted communities to report problems and appeal system outcomes are established and integrated into AI system evaluation metrics.
	4.1	Measurement approaches for identifying AI risks are connected to deployment context(s) and informed through consultation with domain experts and other end users. Approaches are documented.
	4.2	Measurement results regarding AI system trustworthiness in deployment context(s) and across AI lifecycle are informed by input from domain experts and other relevant AI actors to validate whether the system is performing consistently as intended. Results are documented.
	4.3	Measurable performance improvements or declines based on consultations with relevant AI actors including affected communities, and field data about context-relevant risks and trustworthiness characteristics, are identified and documented.

ETSI IoT Framework Controls

Table 5.16

ETSI - Critical Security Controls for IoT

Clause Number	Title	Reference	Status	Detail
5	Reporting implementation	Provision 5.0 1	M	A justification must be recorded for each recommendation considered not applicable. Threat modelling is recommended.
5.1	No universal default passwords	Provision 5.1 1	M	Universal default passwords should not exist on devices.
5.1		Provision 5.1 2	M	Strong password guidelines must be enforced to mitigate risks.
5.1		Provision 5.1 2A	R	It is advisable to periodically review and update password policies.
5.1		Provision 5.1 3	M	Password-related policies must meet minimum strength requirements.
5.1		Provision 5.1 4	M	Devices must have mechanisms for generating unique passwords.
5.1		Provision 5.1 5	M	Unique, pre-installed passwords are necessary; fulfillments depend on conditions.
5.2	Implement a means to manage reports of vulnerabilities	Provision 5.2 1	M	A vulnerability disclosure policy must be made publicly available, including contact info and timelines.
5.2		Provision 5.2 2	R	Companies are encouraged to have clear reporting mechanisms for vulnerabilities.
5.2		Provision 5.2 3	R	Sharing information about vulnerabilities within the industry is advantageous.

5.3	Keep software updated	Provision 5.3 1	R	Regular updates are recommended to maintain security.
5.3		Provision 5.3 2	M	There must be mechanisms to perform timely software updates; details depend on conditions met.
5.3		Provision 5.3 3	M	Timely software updates are mandatory to address security vulnerabilities.
5.3		Provision 5.3 4A	R	Additional measures for conducting updates are recommended.
5.3		Provision 5.3 4B	R	Guidelines for managing specific patches should be adhered to.
5.3	Keep software updated	Provision 5.3 5	R	Manufacturers should facilitate functionalities for automatically updating software where feasible.
5.3		Provision 5.3 6A	R	Recommendations focus on measures to handle updates that require user intervention.
5.3		Provision 5.3 6B	R	Advisable to provide explanations to users regarding the significance of updates.
5.3		Provision 5.3 7	M	Mandatory verification of authenticity and integrity for software updates should occur.
5.3		Provision 5.3 8	M	For updates requiring network delivery, provisions exist to verify trust relationships.
5.3		Provision 5.3 9	R	Recommendations encouraging timely updates for vulnerabilities should be provided.
5.3		Provision 5.3 10	M	Mandatory that updates delivered over the network must undergo authenticity and integrity checks.
5.3		Provision 5.3 11	R	Users should be informed clearly about required

				security updates and associated risks.
5.3		Provision 5.3 12	R	Users must be notified of any updates that may disrupt the device's basic functioning, including expected downtime.
5.3		Provision 5.3 13	M	Manufacturers shall publish clear information regarding the support period for software updates.
5.4	Securely store sensitive security parameters	Provision 5.4 1	M	Mandatory that sensitive security parameters must be securely stored.
5.4		Provision 5.4 2	M	Protect stored sensitive information using strong encryption methods.
5.4		Provision 5.4 3	M	Integrity of security parameters must be continually validated.
5.4		Provision 5.4 4	M	Mechanisms should exist to require access controls for sensitive data.
5.5	Communicate securely	Provision 5.5 1	M	Secure communication methods must be implemented.
5.5		Provision 5.5 2	R	Recommendations on securing communication channels between devices.
5.5		Provision 5.5 3	R	Best practices for secure data exchange between devices should be promoted.
5.5		Provision 5.5 4	R	Communication protocols should be reviewed for security vulnerabilities.
5.5		Provision 5.5 5	M	Mandatory requirement for implementing encrypted communications.
5.5		Provision 5.5 6	R	Recommendations for ensuring data integrity during transmission.
5.5		Provision 5.5 7	M	Mandatory requirement for ensuring that authentication measures are applied.

5.5		Provision 5.5 8	M	Secure data transfer procedures should be established.
5.6	Minimize exposed attack surfaces	Provision 5.6 1	M	Mandatory minimization of interfaces that can be attacked by external entities.
5.6		Provision 5.6 2	M	Reduce the attack surface by limiting the functionalities exposed to the public.
5.6		Provision 5.6 3	R	Recommendations for assessing potential vulnerabilities in different interfaces.
5.6		Provision 5.6 4A	M	Mandatory measures for identifying and documenting all interfaces.
5.6		Provision 5.6 4B	R	Best practices for securing exposed interfaces should be followed.
5.6		Provision 5.6 5	R	Recommendations to implement regular testing of interfaces to check for vulnerabilities.
5.6		Provision 5.6 6	R	Continuous monitoring of exposed interfaces is essential.
5.6		Provision 5.6 7	R	Regular reviews and updates should be made to exposed services to enhance security.
5.6		Provision 5.6 8	R	Recommendations for closing unused interfaces to reduce vulnerabilities should be adopted.
5.6		Provision 5.6 9	R	Ensure permissions are minimized to reduce exposure to attacks.
5.7	Ensure software integrity	Provision 5.7 1	R	Recommendations for verifying software integrity should be established.
5.7		Provision 5.7 2	R	Recommendations on implementing methods for verifying the integrity of software should be noted.
5.8	Ensure that personal data is secure	Provision 5.8 1	R	Recommendations for incorporating privacy-by-design principles into product

				development should be considered.

Each notation means:

- **M (Mandatory)**: This provision is a mandatory requirement that must be implemented.
- **R (Recommendation)**: This provision is recommended, but not required. It suggests best practices or approaches that are advisable to follow.
- **C (Conditional)**: This provision is conditional on certain criteria being met. If the condition is not satisfied, the provision may not apply, and it's marked as N/A (Not Applicable).
- **F (Feature)**: This indicates that the provision applies to a specific feature, capability, or mechanism. The existence of this feature is not deemed mandatory or recommended by the provision. If the feature is absent, it can be marked as N/A.

Appendix D "Strategies For ET & Integrated-Unified Framework "

Strategy for Emerging Technology Adoption

The Emerging Technology Adoption Plan & Strategy focuses on the need for a clear strategy to adopt emerging technologies. As these bring novelty, they introduce associated risks & challenges for businesses; on the other hand, they are also used to solving business problems. Emerging technology adoption should include a proper integration/implementation plan and a testing strategy, ensuring that sufficient test cases are covered to validate the solution against all issues & vulnerabilities. Furthermore, the solution needs to be monitored for performance using defined metrics to support resource optimization & maintenance.

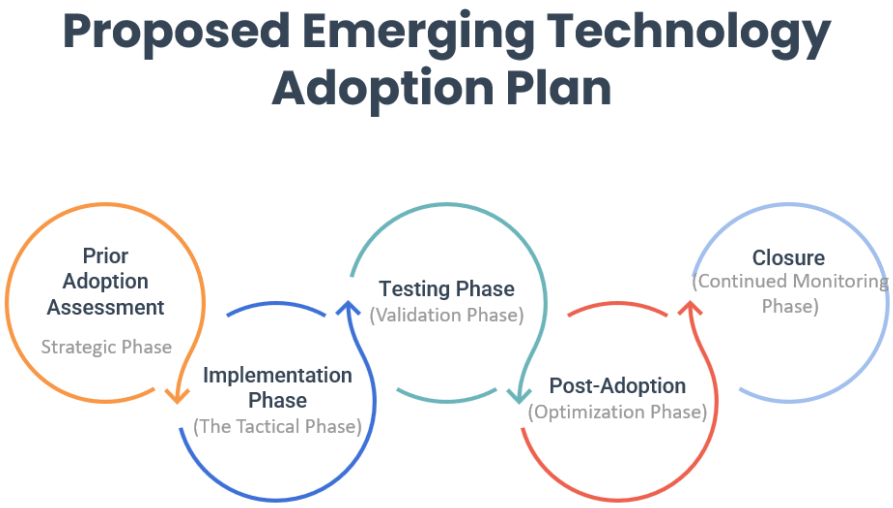


Figure 5.10

ET Adoption Plan for an Enterprise

More than just a plan, a detailed strategy helps ensure any such adoption yields greater results and aligns with the organization's vision, mission & value statements.

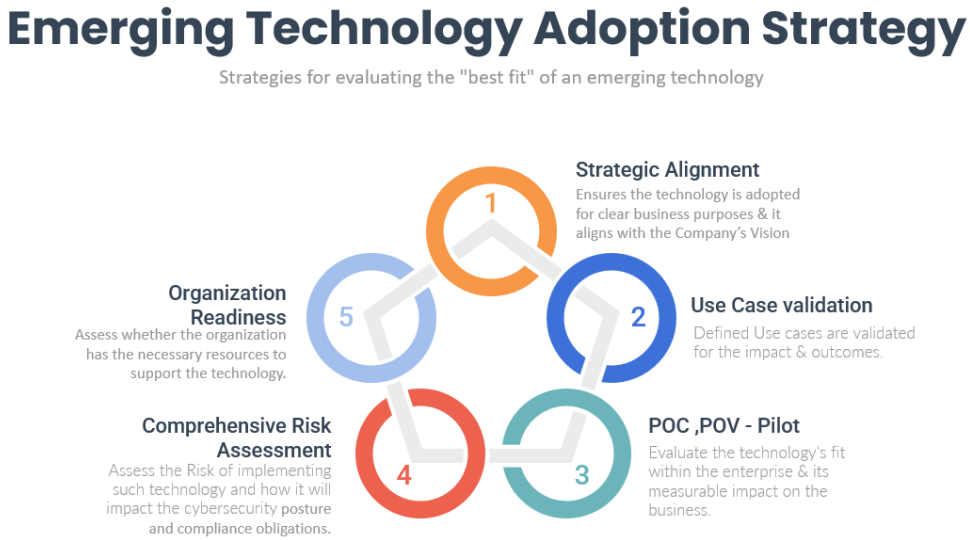


Figure 5.11

ET Adoption Strategy for an Enterprise

High level & Low level strategies have to developed for each of the stage of ET adoption, starting from understanding the technology that is being adopted, organization's readiness to such technology, if the existing resources can support such new technology initiatives, from

alignment with enterprise vision & mission statements along with business objectives to developing use cases of business to ensuring those use cases are achievable through such Emerging technology adoption, further carrying out a technical proof of concepts to be able to measure the impact on Business, along with assessing the risks such technology bring into business & the stake holders, along with the new set of vulnerabilities that could affect the security posture of the organization.

D.1 Unified AI framework

The unified framework table below combines the core functions of the NIST AI Risk Management Framework (AI RMF) with the life cycle stages of ISO/IEC 23053:2021.

Table 5.17

Unified AI Framework

Unified Framework Stage		NIST AI RMF Function	ISO/IEC 23053:2021 Life Cycle Stage
1	Governance & Conception	**GOVERN**	Conception
2	Risk Mapping & Design	**MAP**	Design and Development
3	Measurement & Verification	**MEASURE**	Verification & Validation (V&V)
4	Management & Deployment	**MANAGE**	Deployment
5	Ongoing Oversight & Operation	**MANAGE**	Operation & Monitoring

Note: The framework above is derived from the existing framework by merging the ISO and NIST AI RMF; the controls will be finalized once the Survey Questionnaires are completed and the statistical analysis results are available.

By combining the risk-based approach provided by NIST with the structured life-cycle methodology of ISO, we ensure that AI governance and risk management are treated as a unified process, rather than as separate tasks. They are embedded directly into every stage of the AI system's development and operation, encouraging a culture of proactive and continuous responsibility from conception to retirement. This cohesive, unified model should provide a

clear, actionable roadmap for organizations to manage AI trustworthiness and safety comprehensively.

Table 5.18

AI Strategic Priority

Strategic Priority	**Target Variable**	**Recommendation**	**Framework Alignment**
Culture Building	**Moderator (Leadership)**	Mandatory AI/IoT security training for non-technical executives.	NIST CSF 2.0
Risk Baseline	**Mediator (Framework)**	Conduct a gap analysis between existing ISO controls and the NIST AI RMF or use the Unified Framework to ensure no Gaps in the assessment.	NIST AI RMF
Technical Défense	**IV (Adoption/Depth)**	Deploy automated scanning for OWASP Top 10 vulnerabilities in all LLM apps.	OWASP LLM Top 10
Resilience Planning	**DV (Posture)**	Move from "static" security policies to "adaptive" monitoring.	NIST CSF 2.0

Unified framework combining NIST AI RMF & ISO provides the unification benefits bringing together NIST's AI RMF core functions (Govern–Map–Measure–Manage) with ISO/IEC lifecycle staging to create a more complete, end-to-end view of AI risk, from design through deployment and retirement, aligning a functional, outcome-oriented, sociotechnical risk lens (NIST) with lifecycle-based engineering structure (ISO) helps ensure that governance, measurement, and mitigation activities are systematically embedded at every stage rather than treated as ad hoc add-ons.

We need to make sure all these frameworks have a feedback method to learn & evolve themselves.

An alternative to this could be AI Controls Matrix (AICM) from Cloud Security Alliance, as it maps itself to leading frameworks like ISO 42001, ISO 27001, NIST AI RMF 1.0, and BSI

AIC4, with around 243 controls grouped under five critical pillars like Control Type, Control Applicability and Ownership, Architectural Relevance, LLM Lifecycle Relevance, and Threat Category (“AI Controls Matrix | Framework for Trustworthy AI | CSA,” 2025).

Table 5.19

Unified Framework Stages & Key activities

Unified Framework Stage's	**Key Activities & Controls**
Governance & Conception	•**Establish Foundational AI Governance:** Define and formalize policies for data privacy, bias mitigation, and the responsible use of AI. This includes aligning the project's purpose with legal, ethical, and organizational requirements. •**Define Scope & Stakeholder Accountability:** Clearly document the AI system's purpose, intended use, and limitations. Concurrently, identify key stakeholders and assign clear roles and responsibilities to ensure accountability for the system's actions and outcomes from the outset. • **Conduct Stakeholder Analysis:** Proactively identify and engage with all relevant stakeholders to gather their concerns and feedback, ensuring their perspectives are incorporated into the system's design and risk management plan.
Risk Mapping & Design	•**Conduct Proactive Threat Modelling:** Identify specific threats, vulnerabilities, and potential harms relevant to the AI system. Map the project's design against known attack vectors, such as those from the OWASP Top 10, and proactively design defenses to mitigate them. •**Implement Secure Data Pipelines:** Implement robust data management controls for data quality, security, and privacy. Design a secure data pipeline with validation and sanitization processes to prevent data poisoning. •**Design for Trust and Explainability:** Integrate controls for robustness, reliability, safety, and fairness directly into the system's architecture. Incorporate methods to ensure transparency and explainability of model decisions, building trust in the system's outcomes. •**Secure Input & Output Handling:** Design the system to handle unexpected or malicious inputs and validate all

	model outputs to mitigate injection and other related attacks.
Measurement & Verification	•**Comprehensive Performance and Reliability Testing:** Develop and apply a suite of quantitative metrics to rigorously measure the AI system's performance, reliability, and accuracy under various conditions. This ensures the model functions as expected and consistently meets its operational requirements. • **Systematic Bias and Fairness Audits:** Conduct systematic evaluations to detect and mitigate potential biases and unintended behaviors within the model. This includes using established fairness metrics to ensure the system's outputs are equitable and do not perpetuate or amplify existing societal biases. •**Adversarial & Penetration Testing:** Perform advanced adversarial testing, including red teaming exercises, to simulate sophisticated attacks like prompt injection and data poisoning. This process rigorously evaluates the system's resilience to malicious input and attempts to subvert its intended function. •**Secure Code and Component Analysis:** Conduct thorough security audits and source code reviews of both custom code and all third-party components (e.g., plugins, libraries). This is essential for identifying and remediating vulnerabilities, security flaws, and insecure dependencies before deployment. •**Explainability & Transparency Validation:** Verify that the model's explanations are accurate, consistent, and understandable. This validation process confirms that the system adheres to its designed transparency principles, allowing for effective auditing and stakeholder trust.
Management & Deployment	• Secure Configuration: Harden the deployment environment and API endpoints to prevent attacks. • Rate Limiting: Implement measures to prevent denial-of-service attacks. • Privilege Control: Deploy the model with the minimum necessary privileges to mitigate excessive agency. • Final Vetting: Perform a final security check and vulnerability scan before go-live.

Ongoing Oversight & Operation	• Continuous Monitoring: Implement real-time monitoring for security anomalies and model performance drift. • Audit & Logging: Maintain comprehensive logs to support incident investigation and accountability. • Incident Response: Execute an AI-specific incident response plan for security breaches or unexpected model behavior. • Governance Review: Periodically review the system's impact to ensure it continues to align with ethical and societal values.

Table 5.20

Unified Framework - NIST AI RMF & ISO 23053

Unified Framework Stage's	**NIST AI RMF Function**	**ISO/IEC 23053:2021 Life Cycle Stage**	**Key Activities & Controls**	**Description**
1. Governance & Conception	GOVERN	Conception	• Establish Policies: Define legal, ethical, and organizational requirements for AI systems. • Define Scope: Clearly document the purpose, intended use, and limitations of the AI system. • Assign Roles: Identify and assign roles and responsibilities for AI risk management. • Stakeholder Analysis: Identify and engage with key stakeholders and their concerns.	This initial stage is about establishing the foundational structure, policies, and project scope needed to manage AI risks from the very beginning.

2. Risk Mapping & Design	MAP	Design and Development	• Contextualize Risks: Identify specific threats, vulnerabilities, and potential harms relevant to the AI system's context. • Data Management: Implement controls for data quality, security, and privacy. • Design for Trust: Integrate controls for robustness, reliability, safety, and fairness directly into the system architecture. • Threat Modelling: Perform threat modelling to identify and address potential attack vectors (e.g., prompt injection, data poisoning).	This is where high-level governance is translated into concrete design choices. Risks are identified, mapped, and mitigated through proactive engineering controls.
3. Measurement & Verification	MEASURE	Verification & Validation (V&V)	• Performance Metrics: Develop and use metrics to measure AI system performance, fairness, and reliability. • Testing: Conduct comprehensive security testing, including vulnerability assessments and red teaming. • Bias Audits: Systematically evaluate the model for potential biases	This stage is dedicated to rigorous and systematic testing to confirm that the AI system meets its design objectives and that risk mitigation controls are functioning as intended.

			and unintended behaviours. • Source Code Review: Review custom code and third-party components for security flaws and vulnerabilities.	
4. Management & Deployment	MANAGE	Deployment	• Risk Remediation: Address and prioritize any risks identified during the V&V stage before deployment. • Secure Deployment: Establish a secure process for deploying the AI system to its operational environment. • Access Control: Implement robust access controls and security measures for the deployed system. • Incident Response Plan: Ensure the incident response playbook is updated with AI-specific scenarios.	This stage focuses on the secure and managed transition of the AI system into production, with a clear focus on activating ongoing risk management and incident readiness.
5. Ongoing Oversight & Operation	MANAGE	Operation & Monitoring	• Continuous Monitoring: Implement a continuous monitoring program to track system performance, security, and integrity.	This is the final and continuous stage where the deployed AI system is actively managed, monitored, and maintained until the end of its life cycle.

			• Logging & Auditing: Collect comprehensive logs and audit trails to support incident analysis and accountability. • Incident Response: Execute the AI-specific incident response plan when a security event or failure occurs. • Decommissioning: Establish a formal, secure process for safely decommissioning and retiring the AI system.	

The framework above is derived by merging the ISO & NIST AI RMF.

D.2 Unified IoT Framework

Table 5.21

Unified IOT Critical Controls Table

Unified IOT framework - Critical Controls

Sl. No	Audit Steps	Control ID	Ref Control ID	Control Name	Control Description	Control Maturity	Control Frequency	Control Type	Mapped Frameworks
1	Asset Inventory Validation	UIOT-AM-01	CSF-ID.AM-1	IoT Asset Identification	Maintain an inventory of all IoT devices connected to the network. Deploy automated asset discovery tools, tag and classify devices, and integrate with CMDB.	Advanced	Quarterly	Preventive	NIST CSF, NIST IR 8259, ISO/IEC 27001
2	Firmware Integrity Check	UIOT-FV-02	SP800-53-SI-7	Firmware Validation	Ensure firmware is signed and verified before deployment. Enforce digital signing, validate firmware using hash checks, and maintain a secure repository.	Intermediate	Monthly	Detective	NIST SP 800-53, IoTSF, OWASP IoT Top 10
3	Device Authentication	UIOT-DAU-03	IR8259-DA-1	Secure Device Onboarding	Authenticate devices before granting network access. Use certificate-based authentication, secure boot, and MAC address whitelisting.	Advanced	Real-time	Preventive	NIST IR 8259, CSA IoT, ISO/IEC 27001
4	Threat Modeling	UIOT-TM-04	OWASP-TM-1	IoT Threat Identification	Conduct threat modeling during design phase using STRIDE or PASTA. Document threat scenarios and mitigation strategies.	Basic	Annually	Preventive	OWASP IoT Top 10, MITRE ATT&CK
5	Network Segmentation	UIOT-NS-05	CSF-PR.AC-5	Segmented IoT Zones	Isolate IoT devices from critical systems using VLANs, micro-segmentation, and SDN. Monitor inter-zone traffic.	Advanced	Continuous	Preventive	NIST CSF, ISO/IEC 27001, CMMC
6	Incident Response Planning	UIOT-IRP-06	CSF-RS.RP-1	IoT Incident Response	Develop and test incident response plans for IoT breaches. Conduct exercises and integrate logs into SIEM.	Intermediate	Semi-Annual	Corrective	NIST CSF, CSA IoT, CMMC
7	Data Encryption	UIOT-DE-07	SP800-53-SC-12	IoT Data Protection	Encrypt data at rest and in transit using TLS 1.3 and AES-256. Implement key rotation and secure key management.	Advanced	Continuous	Preventive	NIST SP 800-53, ISO/IEC 27001
8	Supply Chain Risk Management	UIOT-SCRM-08	CSF-GV.SC-1	Vendor Risk Assessment	Evaluate third-party IoT vendors for security compliance. Use questionnaires, require standards compliance, and monitor performance.	Intermediate	Quarterly	Preventive	NIST CSF, CMMC, CSA IoT
9	Logging and Monitoring	UIOT-LM-09	CSA-LOG-1	IoT Activity Monitoring	Implement centralized logging and anomaly detection. Use traffic analysis and correlate with threat intelligence.	Advanced	Continuous	Detective	CSA IoT, MITRE ATT&CK, NIST CSF
10	Patch Management	UIOT-PM-10	IoTSF-PM-1	IoT Patch Lifecycle	Ensure timely patching of IoT firmware and software. Maintain inventory, test patches, and automate deployment.	Basic	Monthly	Corrective	IoTSF, NIST SP 800-53

Table 5.22

Unified IOT Framework/Controls Implementation Steps

Unified IOT implementation Framework				
Framework Component	**Objective**	**Implementation Steps**	**Mapped Frameworks**	**Best Practice**
1. IoT Asset Identification	Maintain a complete inventory of all IoT devices.	Deploy automated asset discovery tools. Tag and classify devices by function, location, and risk profile. Integrate with CMDB (Configuration Management Database).	NIST CSF, NIST IR 8259, ISO/IEC 27001	Use dynamic inventory updates and reconcile with procurement records.
2. Firmware Integrity Check	Ensure firmware authenticity and integrity.	Enforce digital signing of firmware. Validate firmware before deployment using hash checks. Maintain a secure firmware repository.	NIST SP 800-53, IoTSF, OWASP IoT Top 10	Automate firmware validation in CI/CD pipelines.
3. Secure Device Onboarding	Authenticate devices before network access.	Use certificate-based authentication or TPM (Trusted Platform Module). Implement zero-touch provisioning with secure boot. Enforce MAC address whitelisting and identity verification.	NIST IR 8259, CSA IoT, ISO/IEC 27001	Integrate onboarding with IAM (Identity and Access Management).
4. IoT Threat Identification	Identify potential threats during design.	Conduct STRIDE or PASTA threat modeling. Use OWASP IoT Top 10 as a baseline. Document threat scenarios and mitigation strategies.	OWASP IoT Top 10, MITRE ATT&CK	Include threat modeling in SDLC (Software Development Life Cycle).
5. Segmented IoT Zones	Isolate IoT devices from critical systems.	Implement VLANs and firewall rules. Use micro-segmentation and SDN (Software Defined Networking). Monitor inter-zone traffic for anomalies.	NIST CSF, ISO/IEC 27001, CMMC	Apply least privilege access across zones.
6. IoT Incident Response	Prepare for and respond to IoT breaches.	Develop IoT-specific playbooks. Conduct tabletop exercises and simulations. Integrate IoT logs into SIEM (Security Information and Event Management).	NIST CSF, CSA IoT, CMMC	Include device isolation and rollback procedures.
7. IoT Data Protection	Encrypt data at rest and in transit.	Use TLS 1.3 for data in transit. Encrypt storage using AES-256. Implement key rotation and secure key management.	NIST SP 800-53, ISO/IEC 27001	Use hardware-based encryption where feasible.
8. Vendor Risk Assessment	Evaluate third-party IoT vendors.	Conduct security questionnaires and audits. Require compliance with ISO/IEC 27001 and CSA IoT. Monitor vendor performance and breach history.	NIST CSF, CMMC, CSA IoT	Include vendor risk in enterprise risk register.
9. IoT Activity Monitoring	Monitor IoT device behavior.	Deploy network traffic analysis tools. Use anomaly detection algorithms. Log device events and correlate with threat intelligence.	CSA IoT, MITRE ATT&CK, NIST CSF	Enable real-time alerts and automated response.
10. IoT Patch Lifecycle	Ensure timely patching of IoT systems.	Maintain patch inventory and schedule. Test patches in sandbox environments. Automate patch deployment with rollback options.	IoTSF, NIST SP 800-53	Prioritize patches based on CVSS scores and exploitability.

Note: The framework above is derived from the existing framework by merging multiple other frameworks; the controls will be finalized once the Survey Questionnaires are completed and the statistical analysis results are available.

D.3 General Blockchain Assessment Framework

Blockchain Security Assessment: Controls, Documents & Evidence

The unified framework provides a comprehensive checklist for evaluating the security of blockchain implementation. It is structured to verify the effectiveness of security controls through a review of documentation, processes, and practical evidence, with each point supported by key industry and academic sources.

1. Business & Process Layer

The business and process layer addresses organizational and operational controls, which extend beyond compliance. Also, it includes process integrity, data privacy & more that govern the use and management of the blockchain.

Business & Process Layer Security Controls checklist

Security Control	Document/Process Check	Evidence/Practice Check
Governance Model & Governing Rules	Review governance charters and consortium agreements defining decision-making protocols for forks and upgrades (Narayanan et al., 2016).	Interview stakeholders to confirm understanding of governance rules. Review records of past governance decisions (e.g., protocol upgrades).
Trusted Intermediary Issues	If a centralized intermediary exists, review contracts and SLAs that define its role, security obligations, and liability (Nakamoto, 2008).	Conduct a third-party security audit of the intermediary's systems to verify no single point of failure exists.
Auditability & Compliance	Review internal and external audit policies. Check for compliance with data privacy regulations (e.g., GDPR) for on-chain data (World Economic Forum, 2020).	Review audit reports and logs. Trace a transaction through its lifecycle to confirm data integrity and immutability.
Actor Identities & On-chain Privacy	Review the identity management framework, including KYC/AML processes for permissioned networks. Assess data classification policies to ensure sensitive data is not stored on-chain (ENISA, 2021).	Verify that only hashed or non-sensitive data is stored on-chain. Review the process for off-chain data management.
Business Continuity & Incident Response	Review the Business Continuity Plan (BCP) and Incident Response (IR) plan for handling security incidents (e.g., 51% attack, smart contract exploit) (NIST, 2018).	Conduct a tabletop exercise of the IR plan. Review logs of past security incidents and the response actions taken.

2. Application Layer

The application layer, as always, focuses on the security of user-facing applications and smart contracts built on the blockchain to support a decentralized system.

Application Layer Control Checklist

Security Control	Document/Process Check	Evidence/Practice Check
Smart Contract Security	Review smart contract code against standards like the OWASP Smart Contract Top 10 for risks such as reentrancy and integer overflows (OWASP, 2023).	Request and review final smart contract audit reports from an independent third party. Conduct automated vulnerability scanning.
Transactional Data Security	Review encryption and digital signature standards used for transactions (Zheng et al., 2017). Check for multi-signature (multisig) policies.	Verify transactions are signed correctly and that private keys are securely managed. Attempt to manipulate a pending transaction to test its integrity.
API & User Interface (UI) Security	Review API documentation and security policies (e.g., API Gateway, authentication tokens). Check for front-end security practices like input validation (ISO, 2020).	Conduct penetration testing on the APIs and UI to check for vulnerabilities like XSS and SQL injection.
Access Control	Review the access control matrix defining which users or smart contracts can perform specific actions (ConsenSys Diligence, 2023).	Verify that access to privileged functions (e.g., token minting, contract upgrades) is restricted and requires a multisig process.

3. Execution Layer (Smart Contracts & Virtual Machines)

This layer concerns the environment in which transactions are processed and smart contracts are carried out.

Execution Layer Control Checklist

Security Control	Document/Process Check	Evidence/Practice Check
Execution Environment Hardening	Review the design document for the blockchain's virtual machine (e.g., EVM). Check for a sandbox environment to isolate smart contract execution (Wood, 2014).	Verify that the virtual machine handles exceptions and errors gracefully to prevent Denial of Service (DoS) attacks.
Transaction Validation Logic	Review the code and documentation for the logic that validates transactions before they are executed.	Submit a malformed or "double-spend" transaction to the network to verify it is rejected by all nodes (Narayanan et al., 2016).
State Transition & Finality	Review the mechanism for updating the blockchain state after a block is added. Check for "settlement finality" to ensure transactions are irreversible (Gervais et al., 2016).	Verify that the chain cannot be forked and that the protocol's finality guarantees are met.

4. Consensus Layer

This layer's security is critical for maintaining the integrity and agreement of the distributed ledger.

Consensus Layer Control Checklist

Security Control	Document/Process Check	Evidence/Practice Check
Consensus Algorithm Resilience	Review the consensus algorithm's resistance to a 51% attack (for PoW) or long-range attacks (for PoS) (Investopedia, 2025).	Conduct stress testing to simulate a majority attack and verify its resilience. Examine the distribution of validator/mining power to ensure it is decentralized.
Byzantine Fault Tolerance (BFT)	Review the protocol's BFT properties and how it handles a specified number of malicious nodes (Bitstamp, 2023).	Simulate node failures and malicious behavior (e.g., withholding blocks) to verify the network continues to operate correctly.
Consensus Participation & Incentives	Review the incentive model (e.g., block rewards, slashing) that encourages honest participation (Investopedia, 2025).	Verify that the reward mechanism is correctly implemented. Review records of any slashing events to confirm penalties were applied.
Energy Efficiency	For Proof of Stake or other non-PoW systems, review the energy consumption reports for validator nodes to confirm efficiency (Investopedia, 2025).	Conduct an energy usage audit on the nodes to compare against expected efficiency metrics.

5. Network Layer

The network layer in Blockchain is focussed towards addressing the security of the peer-to-peer (P2P) network that connects the nodes.

Network Layer Control Checklist

Security Control	Document/Process Check	Evidence/Practice Check
P2P Communication Security	Review the protocol's use of encryption (e.g., TLS) for inter-node communication and authentication (Bitstamp, 2023).	Use network monitoring tools to confirm encrypted communication. Attempt to connect a non-whitelisted node to a permissioned network.
Eclipse & Routing Attack Mitigation	Review the network's design for peer discovery and management, and safeguards against a node being isolated (Startup Defense, 2023).	Simulate an eclipse attack by isolating a node and verify that it can reconnect to the wider network.
Scalability (Client & Validation Nodes)	Review the high-level design to understand the network's scalability solutions (e.g., sharding, Layer 2). Check for latency and throughput metrics (Zheng et al., 2017).	Conduct performance testing to assess the network's throughput under high transaction volume.

6. Data Layer

This Data layer in Blockchain is concerned with the integrity and security of data stored on the blockchain network itself.

Data Layer Control Checklist

Security Control	Document/Process Check	Evidence/Practice Check
Immutability & Cryptographic Hashing	Review the hashing algorithm (e.g., SHA-256) and how it is used to link blocks cryptographically (SciTePress, 2025).	Attempt to modify a transaction in an existing block and verify that it invalidates the hash of the block and all subsequent blocks.
Data Integrity & Provenance	Review the mechanism for data provenance and the ability to trace the history of a digital asset (arXiv, 2024).	Trace a digital asset from its creation to a final state to confirm its entire history is accurately recorded and cannot be falsified.
Data Accessibility & Off-chain Storage	Review policies for data accessibility, including off-chain storage solutions (e.g., IPFS) and their security (World Economic Forum, 2020).	Verify that sensitive data is not on-chain. Test the security of off-chain data stores with a vulnerability scan.

7. Hardware Layer

The Hardware layer in blockchain focuses on the physical and virtual infrastructure that supports the blockchain nodes.

Hardware Layer Control Checklist

Security Control	Document/Process Check	Evidence/Practice Check
Physical & Cloud Security	Review the security policies for data centers or cloud provider infrastructure. Check for access controls, environmental monitoring, and disaster recovery (Revelo, 2023).	Conduct a site visit or review the cloud provider's security audit reports (e.g., SOC 2, ISO 27001).
Hardware Security Modules (HSMs)	Review the use of FIPS-compliant HSMs for key management, especially for validator nodes and multisig wallets (Fortinet, 2024).	Verify that private keys are stored in HSMs. Conduct a test of the key generation and signing processes to ensure they are secure.
Node Security Hardening	Review the baseline security configurations for all nodes. Check for patch management policies, host-based firewalls, and intrusion detection systems (NIST, 2018).	Conduct a vulnerability scan and penetration test on a sample of nodes. Review logs to confirm regular patching and security updates are being applied.

Thank you

"End of this Thesis"