American Journal of Interdisciplinary Studies
Volume 05, Issue 04 (2024)
Page No: 24- 66
Doi: 10.63125/tkvxak20

CYBERSECURITY IN ENTERPRISE INFORMATION SYSTEMS: PREVENTING DATA BREACHES IN THE USA

Sanath Kumar Chebrolu[1]; Sanjai Vudugula[2];

[1]*Management Information System,College of Busines, Lamar University, USA*
Email: chebrolusanath2000@gmail.com

[2]*Master in Management Information System,College of Busines, Lamar University, USA*
Email: sanjaivudugula02@gmail.com

Citation:
Chebrolu, S. K., & Vudugula, S. (2024). *Cybersecurity in enterprise information systems: Preventing data breaches in the USA*. *American Journal of Interdisciplinary Studies, 5*(4), 24–66. https://doi.org/10.63125/tkvxak20

Received:
September 10, 2024

Revised:
October 15, 2024

Accepted:
November 20, 2024

Published:
December 18, 2024

Abstract

This systematic literature review investigates the evolving landscape of cybersecurity practices within enterprise information systems (EIS), with a specific focus on U.S.-based organizations. By analyzing 144 peer-reviewed articles published between 2010 and 2024, the study synthesizes insights across multiple thematic areas, including cybersecurity maturity models, Zero Trust Architecture (ZTA), identity and access management (IAM), incident response planning, cloud security, and governance frameworks. Following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, the review identifies critical gaps between theoretical best practices and real-world implementation. The findings reveal that while conceptual frameworks such as CMMI, CMMC, and NIST CSF are widely acknowledged, their practical adoption remains inconsistent across sectors. Zero Trust Architecture, though increasingly recognized for its benefits, has yet to be fully integrated into enterprise-wide strategies due to technical, organizational, and cultural barriers. Identity and access controls are often fragmented, and incident response plans, where present, are frequently underdeveloped or untested. Furthermore, organizations struggle with securing hybrid and multi-cloud environments and often underutilize benchmarking and governance models, leading to reactive and siloed cybersecurity efforts. The review emphasizes that effective cybersecurity in enterprises requires a holistic, integrated approach that combines technical safeguards with governance, leadership commitment, and continuous adaptation to emerging threats. These findings serve as a foundation for future research and practice, offering actionable insights for strengthening organizational cybersecurity readiness in an era of increasing digital complexity.

Keywords

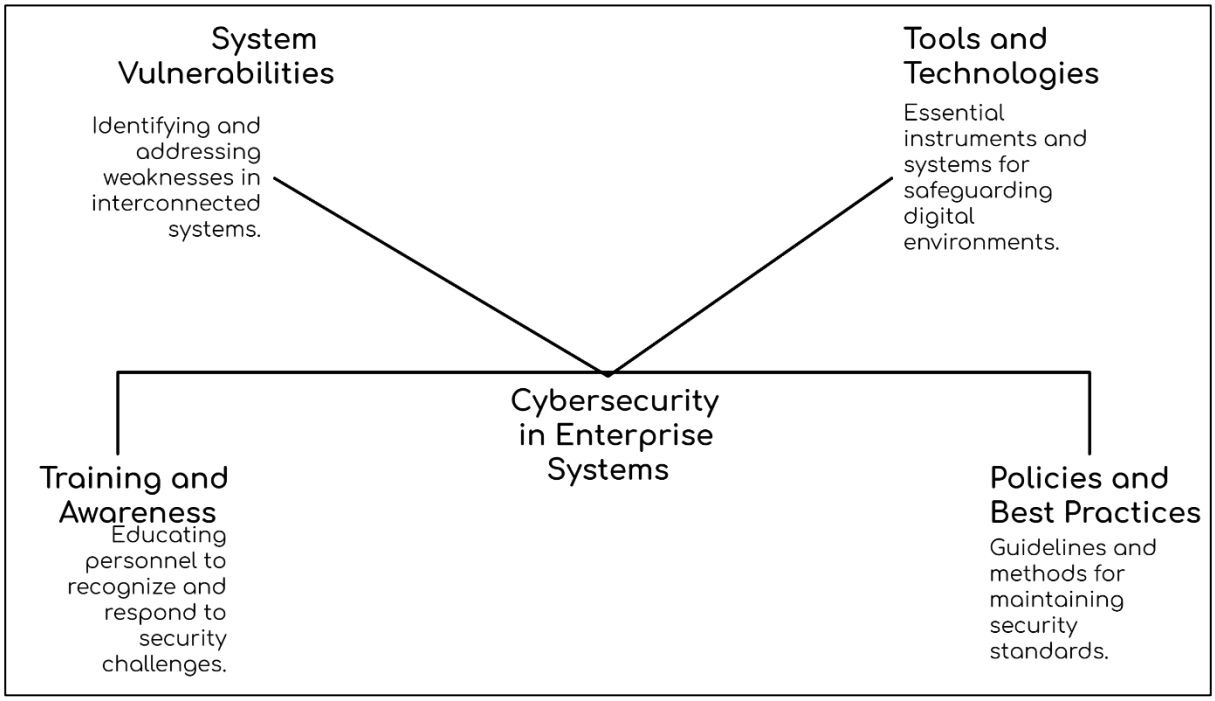
Cybersecurity; Enterprise Information Systems; Data Breach Prevention; Zero Trust Architecture; Information Security Compliance;

American Journal of Interdisciplinary Studies
Volume 05, Issue 04 (2024)
Page No: 24- 66
Doi: 10.63125/tkvxak20

INTRODUCTION

Cybersecurity, broadly defined as the practice of protecting systems, networks, and data from digital attacks, has evolved into a critical area of concern within modern information systems, especially in enterprise settings (Liu et al., 2020). The International Telecommunication Union (ITU) defines cybersecurity as the collection of tools, policies, security concepts, risk management approaches, actions, training, best practices, assurances, and technologies that can be used to protect the cyber environment and organization assets (Buja, 2021). Enterprise Information Systems (EIS), which refer to large-scale software solutions that facilitate the flow of information and coordination of business processes across organizations (Islam et al., 2018), have become pivotal in global business infrastructure. These systems typically include Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), and Supply Chain Management (SCM), all of which process highly sensitive data such as financial records, customer profiles, and operational metrics (Haddad & Binder, 2019). Given their integration across critical business functions, EIS are increasingly becoming targets for sophisticated cyber threats. The global rise in cybercrime, evidenced by the annual increase in reported data breaches, underscores the international relevance of cybersecurity in enterprise environments (Frank et al., 2019; Gordon et al., 2015). Data breaches compromise not only operational continuity but also stakeholder trust and regulatory compliance (Shaikh & Siponen, 2023), reinforcing the importance of securing enterprise systems.

Figure 1: Safeguarding Enterprise Systems Against Evolving Cyber Threats



Cyber threats targeting enterprise environments have become more sophisticated and persistent, leveraging vulnerabilities across interconnected systems and supply chains. According to (Walton et al., 2020), over 60% of enterprises have experienced at least one significant data breach, primarily due to phishing, ransomware, and insider threats. These threats often exploit system vulnerabilities, misconfigured cloud platforms, and outdated software (Lee, 2020). For example, the SolarWinds attack, one of the most significant enterprise-targeted breaches, revealed systemic

vulnerabilities in software supply chains and third-party integrations (Wu & Irwin, 2016). The complexity and size of enterprise systems exacerbate these risks by introducing numerous attack surfaces (Ibrahim et al., 2020). The diversity in enterprise system architectures, which often integrate legacy systems with cloud-based applications, further complicates cybersecurity efforts (Brody et al., 2018). Additionally, the COVID-19 pandemic intensified these challenges by accelerating the shift toward remote work and increasing reliance on digital collaboration platforms, which were not always configured with security in mind (Montasari et al., 2018). These developments highlight the urgency of implementing comprehensive cybersecurity frameworks tailored to enterprise contexts.

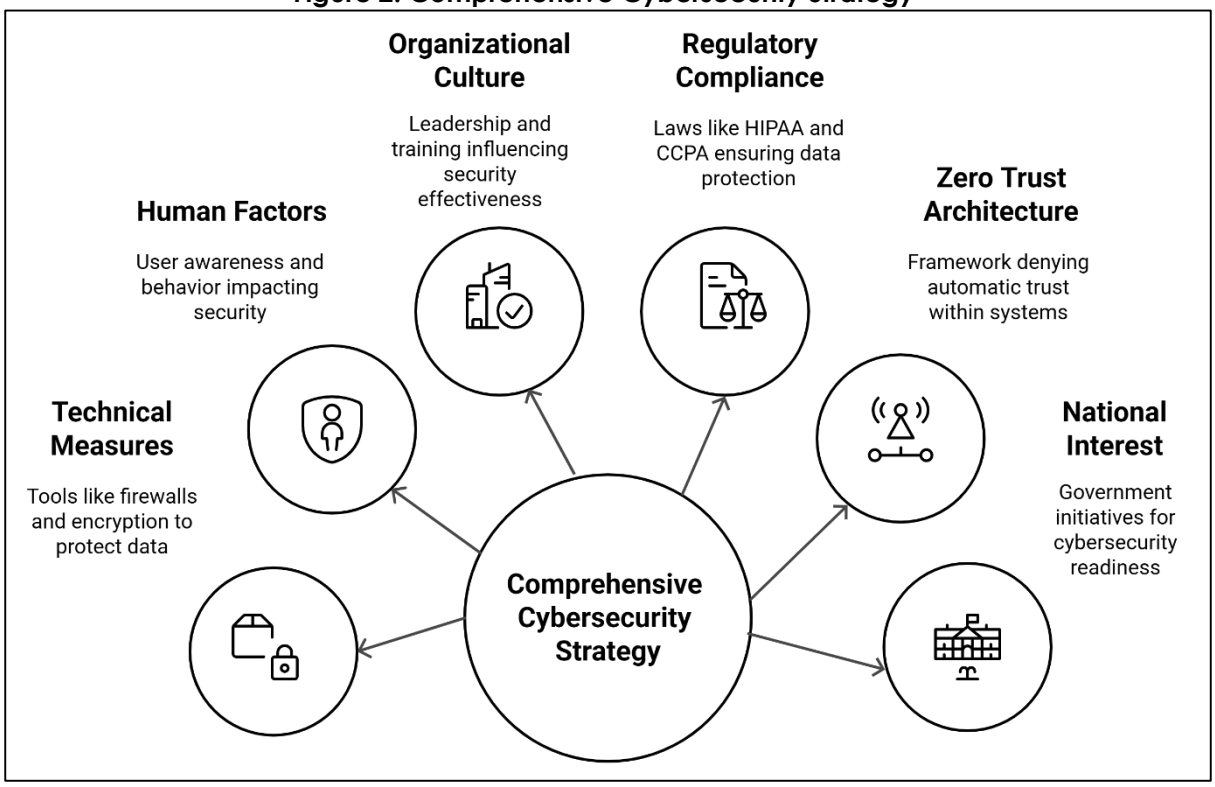
Preventing data breaches in EIS involves addressing a wide spectrum of technical, human, and organizational vulnerabilities. Technical approaches often include deploying firewalls, intrusion detection systems, encryption mechanisms, and secure authentication protocols (Borky & Bradley, 2018). However, technology alone is insufficient in mitigating risks if users lack awareness or follow poor security practices (Algarni et al., 2021). Human factors, including phishing susceptibility and negligent behavior, remain leading causes of data breaches (Benaroch, 2018). Organizational culture and leadership commitment to cybersecurity also significantly affect the effectiveness of security programs (Benaroch, 2018; Walton et al., 2020). Organizations that promote a culture of security awareness, ongoing training, and shared accountability tend to experience lower breach incidents (Lee, 2020). Furthermore, regulatory requirements, such as the Health Insurance Portability and Accountability Act (HIPAA) and California Consumer Privacy Act (CCPA), compel U.S.-based enterprises to adopt stringent cybersecurity controls (Ibrahim et al., 2020). Compliance, however, should not be treated as the endpoint of cybersecurity efforts but as a baseline upon which proactive strategies are built (Wu & Irwin, 2016).

The architecture of modern enterprise systems poses unique challenges to cybersecurity because of their scale, heterogeneity, and constant evolution. Cloud computing, while enabling scalability and flexibility, also introduces risks related to data residency, multi-tenancy, and lack of visibility into third-party infrastructure (Islam et al., 2018). Hybrid enterprise systems combining on-premise and cloud resources create complex environments where standard security measures may not suffice (Haddad & Binder, 2019). Moreover, the trend toward Bring Your Own Device (BYOD) and mobile-first enterprise applications expands the threat landscape, increasing the number of endpoints susceptible to attacks (Frank et al., 2019). Attackers often exploit lateral movement opportunities, gaining unauthorized access to multiple systems once an initial vulnerability is breached (Gordon et al., 2015). To combat this, Zero Trust Architecture has emerged as a robust framework where no user or system is automatically trusted, even if they reside within the enterprise perimeter (Snyder et al., 2015). Studies show that Zero Trust policies significantly reduce breach dwell time and lateral movement success (Shaikh & Siponen, 2023), although implementation across diverse systems remains a challenge (Walton et al., 2020). Within the United States, cybersecurity for EIS is not just a technical concern but a matter of national interest, given the critical role these systems play in economic infrastructure. High-profile breaches such as those experienced by Equifax, Colonial Pipeline, and Target have led to significant financial loss, reputational damage, and disruptions in essential services (Lee, 2020). These incidents have also prompted governmental initiatives to enhance cybersecurity readiness, including the Cybersecurity and Infrastructure Security Agency (CISA) and Executive Orders on improving the nation's cybersecurity posture (Wu & Irwin, 2016). The Biden Administration's cybersecurity strategy calls for

American Journal of Interdisciplinary Studies
Volume 05, Issue 04 (2024)
Page No: 24- 66
Doi: 10.63125/tkvxak20

mandatory breach reporting, greater public-private collaboration, and investment in cybersecurity workforce development (Ibrahim et al., 2020). Regulatory enforcement by the Federal Trade Commission (FTC), Department of Homeland Security (DHS), and Securities and Exchange Commission (SEC) further enforces corporate accountability for data protection (Brody et al., 2018). These developments underscore the importance of integrating cybersecurity strategy into enterprise governance and risk management frameworks (Brody et al., 2018; Montasari et al., 2018).

Figure 2: Comprehensive Cybersecurity Strategy



Cybersecurity in enterprise systems also intersects with risk management, incident response, and business continuity planning. Organizations that lack mature cybersecurity incident response plans often suffer greater financial and operational impacts from data breaches (Borky & Bradley, 2018). Studies show that having a dedicated cybersecurity team and documented response protocol can reduce the average cost of a data breach by 40% (Algarni et al., 2021). Risk assessments tailored to the unique configurations and threat profiles of enterprise systems are essential in identifying critical assets and potential attack vectors (Benaroch, 2018). Additionally, real-time monitoring and behavioral analytics enable early detection of anomalies and insider threats, which account for a significant portion of data breaches in enterprises (Roshanaei, 2021). These capabilities are increasingly powered by machine learning and artificial intelligence, enhancing threat detection accuracy while reducing false positives (Li et al., 2018). However, integrating these advanced tools requires alignment with existing IT and governance structures, necessitating collaboration across departments and leadership support (Bertino, 2016; Li et al., 2018).

The effectiveness of cybersecurity in enterprise information systems depends heavily on maintaining robust compliance with standards and frameworks tailored to enterprise risk levels. The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), International Organization for Standardization (ISO) 27001, and Control Objectives for Information and Related Technologies (COBIT) offer

guidance for establishing security controls aligned with enterprise goals. These frameworks emphasize continuous risk assessment, access control, encryption, network security, and incident response management. However, the adoption and implementation of these standards vary widely among enterprises due to cost constraints, lack of technical expertise, and complexity of system integration (Ter, 2018). Cultural and organizational barriers also hinder cybersecurity maturity, particularly in enterprises where security is not prioritized at the strategic level (Gay, 2017). Education, training, and awareness campaigns are recognized as crucial elements in closing these gaps, as they help establish a shared understanding of risks and responsibilities across the enterprise (Ulven & Wangen, 2021). Therefore, addressing cybersecurity in EIS demands a nuanced understanding of both technological and organizational dimensions in order to effectively reduce the risk of data breaches in enterprise environments. The central objective of this study is to critically analyze and evaluate the existing cybersecurity frameworks, strategies, and practices implemented within enterprise information systems (EIS) in the United States, with a specific focus on identifying their effectiveness in preventing data breaches. To achieve this, the study delineates several key objectives: (1) to identify common cyber threats and attack vectors that target enterprise information systems; (2) to assess the current technical and organizational cybersecurity measures adopted by enterprises; (3) to examine the compliance level of U.S. enterprises with national and international cybersecurity standards and regulations; and (4) to evaluate the role of cybersecurity training, risk governance, and leadership in strengthening data protection within enterprise environments. Through a systematic literature review and synthesis of empirical studies, the research seeks to provide evidence-based insights into how well-prepared enterprises are in defending against cyber threats and minimizing data loss, financial damage, and reputational harm. For instance, the increasing reliance on cloud services, mobile technology, and third-party vendors has introduced new layers of vulnerability, which necessitates detailed investigation into enterprise-level risk assessments and incident response mechanisms. Additionally, the study aims to examine the operationalization and implementation of emerging models such as Zero Trust Architecture (ZTA) and AI-based threat detection systems across various sectors. By mapping these practices to regulatory benchmarks such as the NIST Cybersecurity Framework and HIPAA/CCPA mandates, this study contributes to a structured understanding of best practices and compliance gaps. Furthermore, the study intends to explore organizational behavior factors—such as employee awareness, leadership commitment, and cybersecurity culture—which are often overlooked in purely technical assessments. Ultimately, these objectives guide a comprehensive evaluation of enterprise cybersecurity maturity and reveal actionable pathways for minimizing data breach risks in the U.S. corporate landscape.

LITERATURE REVIEW

In the realm of digital transformation and enterprise system integration, cybersecurity has emerged as a foundational pillar of sustainable business operations and regulatory compliance. Enterprise Information Systems (EIS), comprising technologies such as Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), and Supply Chain Management (SCM), represent mission-critical infrastructures that aggregate and process sensitive corporate and customer data. As these systems grow in complexity and connectivity, so does their vulnerability to cyber threats, necessitating a rigorous investigation of the security mechanisms in place to safeguard enterprise assets. The literature on cybersecurity in EIS spans a wide range of domains—from technical threat mitigation strategies and risk management

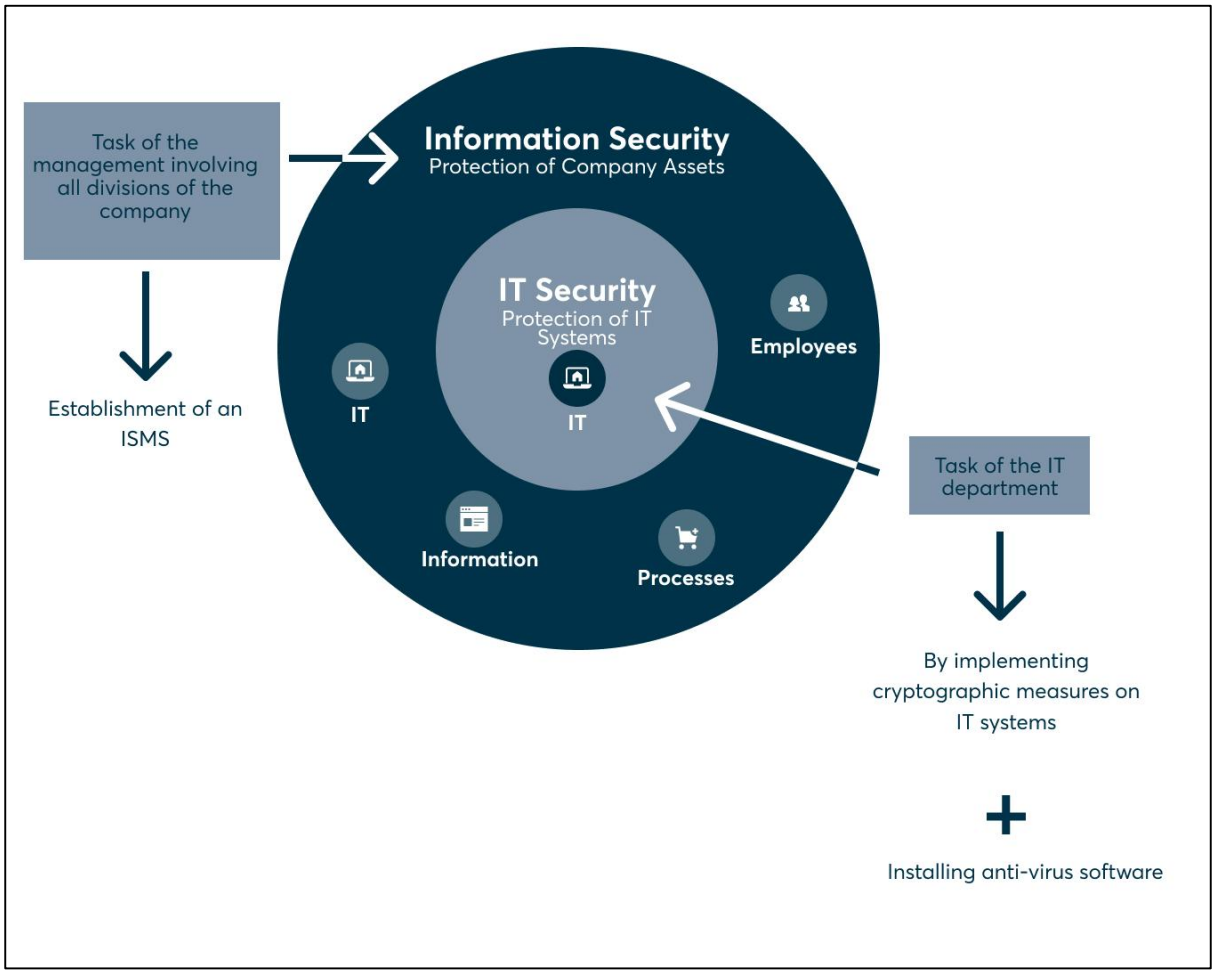
frameworks to organizational behavior, compliance, and governance issues. Recent high-profile breaches in the United States, including those affecting Equifax, Colonial Pipeline, and SolarWinds, underscore the urgent need for comprehensive security postures tailored to large-scale enterprise environments. This literature review seeks to synthesize empirical studies, theoretical frameworks, and industry best practices that inform cybersecurity policies and practices in U.S. enterprises. The purpose of this section is to critically evaluate the multidimensional aspects of cybersecurity in EIS, identify existing gaps, and provide a knowledge base that underpins effective breach prevention strategies. The review is organized into several focused sub-sections addressing threat landscapes, technological defenses, regulatory frameworks, organizational culture, and architectural security models, ensuring a holistic examination of the topic.

Cybersecurity within Enterprise Information Systems

Enterprise Information Systems (EIS) have undergone significant transformations since their initial adoption in the late 20th century, evolving from basic transaction processing systems to sophisticated, integrated platforms supporting real-time operations and decision-making. Historically, early EIS focused on automating back-office functions such as payroll, accounting, and inventory control using mainframe-based systems (Li et al., 2020; Mohiul et al., 2022). These systems operated in closed environments with limited network connectivity, which minimized external security threats. Consequently, security protocols were rudimentary and primarily focused on physical access controls and basic password authentication (Couce-Vieira et al., 2020; Maniruzzaman et al., 2023). The introduction of relational databases in the 1980s and the proliferation of client-server models in the 1990s marked a turning point, enabling enterprises to process and store larger volumes of data across distributed environments (Ahmed et al., 2022; Gordon et al., 2019). As data became more centralized yet accessible, the security focus shifted toward database access control and data integrity measures (Aklima et al., 2022; Liu et al., 2020). With the rise of enterprise resource planning (ERP) systems, such as SAP and Oracle, organizations began to centralize diverse business functions, which increased the attack surface and required more robust cybersecurity protocols (Buja, 2021; Helal, 2022). The early 2000s saw the introduction of network-based security mechanisms, including firewalls, intrusion detection systems (IDS), and antivirus software (Alahmari & Duncan, 2020; Mahfuj et al., 2022). These tools, while effective in static environments, struggled to adapt to rapidly changing threats in dynamic enterprise settings (Majharul et al., 2022; Szádeczky, 2018). Researchers have noted that traditional perimeter-based security models often failed to provide adequate protection against internal threats and advanced persistent threats (APTs) (Berkman et al., 2018; Hossen & Atiqur, 2022; Szádeczky, 2018). Over time, the cybersecurity approach within EIS matured into a more layered defense model involving encryption, secure protocols (e.g., SSL/TLS), and policy-driven access control mechanisms (Mishra et al., 2022; Mohiul et al., 2022). This evolution underscores the reactive nature of early security strategies, where protections were developed incrementally in response to emerging threats rather than through anticipatory design.

American Journal of Interdisciplinary Studies
Volume 05, Issue 04 (2024)
Page No: 24- 66
Doi: 10.63125/tkvxak20

Figure 3: Relationship Between Information Security and IT Security in an Enterprise Environment



Source: www.dataguard.com (2024)

The transition from isolated, standalone enterprise systems to interconnected networks marked a paradigm shift in how businesses managed data, collaboration, and digital infrastructure. In earlier implementations, enterprise systems operated in siloed configurations with minimal interaction between departments or external systems (Haapamäki & Sihvonen, 2019; Kumar et al., 2022). These configurations, though limited in functionality, offered inherent protection by virtue of their isolation. However, the demand for real-time data access, supply chain integration, and customer responsiveness led to widespread adoption of networked EIS solutions (Bodin et al., 2018; Sohel et al., 2022). With the rise of the internet and enterprise intranets in the late 1990s and early 2000s, organizations began linking ERP, CRM, and SCM systems across geographically dispersed sites, introducing vulnerabilities previously absent in standalone systems (Tissir et al., 2020; Tonoy, 2022). Integration with vendor platforms, third-party APIs, and cloud services exposed critical infrastructure to new threat vectors, such as man-in-the-middle attacks, injection attacks, and data exfiltration (Bodin et al., 2018; Tissir et al., 2020; Younus, 2022). Studies have shown that interconnected systems suffer from shared security liabilities, where a breach in one node can cascade across the network (Alam et al., 2023; Hatcher et al., 2020). These risks are compounded by the increased complexity of IT ecosystems, which include diverse technologies, legacy systems, and decentralized control over endpoints (Arafat Bin et al., 2023; Nolan et al., 2019). Furthermore, the expansion of mobile computing and Bring Your Own Device (BYOD) policies further blurred network

perimeters, rendering traditional perimeter defenses insufficient (Alshaikh, 2020; Chowdhury et al., 2023). In response, cybersecurity frameworks such as Defense-in-Depth and the use of Intrusion Prevention Systems (IPS) and Data Loss Prevention (DLP) tools became prevalent (Alshaikh, 2020; Jahan, 2023; Kelton & Pennington, 2019). Nevertheless, research indicates that enterprises still face difficulties in enforcing consistent security policies across interconnected systems, leading to security gaps exploitable by both external actors and insiders (Mahdy et al., 2023; Romanosky, 2016).

As enterprise environments evolved into digital ecosystems powered by real-time data exchange, cloud computing, and automation, the need for integrated cybersecurity within enterprise information systems became increasingly apparent (Maniruzzaman et al., 2023). Unlike legacy systems where cybersecurity was often an afterthought, modern EIS are now being designed with embedded security features that span applications, databases, and networks (Islam et al., 2018; Hossen et al., 2023). Integrated cybersecurity refers to the alignment of security mechanisms with the core architecture of enterprise systems, enabling continuous monitoring, threat detection, and policy enforcement without disrupting business operations (Haddad & Binder, 2019; Roksana, 2023). The shift towards integration has been facilitated by advances in artificial intelligence (AI) and machine learning (ML), which enhance anomaly detection and predictive analytics in identifying potential threats (Haddad & Binder, 2019; Islam et al., 2018; Shahan et al., 2023). For instance, behavioral analytics tools can monitor user activity across EIS platforms and trigger alerts for deviations from established patterns (Frank et al., 2019; Tonoy & Khan, 2023). Moreover, integrated security frameworks such as Zero Trust Architecture (ZTA) have gained traction in enterprise settings, focusing on identity verification, micro-segmentation, and least privilege access to minimize breach impact (Al-Arafat, Kabi, et al., 2024; Frank et al., 2019; Gordon et al., 2015). These models challenge the assumption of internal network trust, which has historically led to blind spots in cybersecurity strategy (Al-Arafat, Kabir, et al., 2024; Snyder et al., 2015). Additionally, enterprise-wide adoption of Identity and Access Management (IAM) and encryption standards such as TLS/SSL have become integral components of secure infrastructure. Studies have shown that companies with integrated cybersecurity frameworks report lower incident response times and reduced data breach costs compared to those relying on fragmented security solutions (Alam et al., 2024; Shaikh & Siponen, 2023). Furthermore, compliance requirements under HIPAA, CCPA, and the General Data Protection Regulation (GDPR) increasingly demand systemic, rather than piecemeal, approaches to data protection (Alam et al., 2024; Shaikh & Siponen, 2023). Integrated cybersecurity thus represents a strategic evolution in enterprise defense—embedding security within the very fabric of digital business operations.

Integrating cybersecurity into enterprise information systems introduces a unique set of interdisciplinary challenges that span technical, organizational, and human dimensions (Ammar et al., 2024). Unlike isolated security implementations that focus solely on firewalls or encryption, embedded security requires cross-functional collaboration between IT teams, business process owners, compliance officers, and executive leadership (Bhowmick & Shipu, 2024; Walton et al., 2020). This integration is often hindered by misalignment between security protocols and business objectives, where cybersecurity is viewed as a cost center rather than a strategic enabler (Bhuiyan et al., 2024; Lee, 2020). Studies have shown that enterprises struggle to incorporate cybersecurity considerations into system development lifecycles (SDLC), resulting in vulnerabilities that are only addressed after deployment (Dasgupta &

Islam, 2024; Wu & Irwin, 2016). Moreover, the lack of standardized metrics to assess cybersecurity maturity within EIS creates inconsistencies in how risks are prioritized and mitigated (Dey et al., 2024; Ibrahim et al., 2020). The challenge is compounded by the rapid evolution of threat landscapes, where static controls may become obsolete within months (Brody et al., 2018; Hasan et al., 2024). Human factors continue to be a dominant concern, as employee negligence and poor password hygiene remain among the top causes of enterprise data breaches (Haddad & Binder, 2019; Helal, 2024). Despite ongoing training initiatives, organizations face resistance to behavioral change, especially when security practices are perceived to impede productivity (Frank et al., 2019; Hossain et al., 2024). Additionally, implementing advanced tools like AI-based detection or ZTA requires significant investment and specialized skillsets, which are often lacking in mid-sized organizations (Haddad & Binder, 2019; Hossain et al., 2024). These interdisciplinary barriers highlight the need for enterprise-wide security governance models that embed cybersecurity into organizational culture, process design, and executive accountability structures (Haddad & Binder, 2019; Islam, 2024; Romanosky, 2016).

Threat Vectors and Attack Surfaces in U.S. Enterprises

Cyberattacks targeting Enterprise Information Systems (EIS) in the U.S. have grown in complexity, scope, and impact, exposing sensitive business data and disrupting critical operations. Among the most prevalent attack vectors are phishing, malware, ransomware, and advanced persistent threats (APTs). Phishing attacks, typically leveraging deceptive emails to gain user credentials or install malicious payloads, are responsible for over 90% of successful breaches in enterprise environments (Frank et al., 2019; Gordon et al., 2015; Islam et al., 2024). Fielder et al. (2016) emphasize that employee awareness and training are critical in mitigating phishing risks, yet many organizations underestimate their significance. Malware, including Trojans and spyware, remains a persistent threat to enterprise networks, exploiting outdated software and unpatched vulnerabilities (Cavusoglu et al., 2008; Fielder et al., 2016). Ransomware attacks, which encrypt critical files and demand payment for decryption keys, have surged in recent years, crippling public and private institutions alike (Da Veiga et al., 2020; Islam, 2024). APTs represent a more sophisticated class of threat, characterized by stealthy and prolonged infiltration designed to exfiltrate valuable information without detection (Jahan, 2024; Kamra et al., 2007). These threats often utilize zero-day vulnerabilities, privilege escalation, and lateral movement to compromise multiple systems within the enterprise (Fang et al., 2012; Jim et al., 2024; Kamra et al., 2007). The interconnected nature of modern EIS platforms, especially in cloud-based and hybrid deployments, further complicates threat detection and containment (Alsowail & Al-Shehari, 2020; Khan & Aleem Al Razee, 2024). Moreover, social engineering attacks increasingly exploit trust-based relationships within enterprises to bypass technical controls (Cheng et al., 2017; Mahabub, Das, et al., 2024). Collectively, these studies illustrate that no single technical defense is sufficient; instead, a multi-layered cybersecurity framework that includes real-time monitoring, behavior analytics, and user training is essential for safeguarding enterprise systems from diverse attack vectors.

Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), and Supply Chain Management (SCM) platforms represent the backbone of modern enterprises, yet they harbor substantial vulnerabilities that cyber attackers frequently exploit. ERP systems, due to their extensive integration across business functions, are particularly attractive targets. Researchers note that many ERP applications, especially older ones, lack robust access control and are often not patched regularly

due to operational complexity (Magklaras & Furnell, 2001; Mahabub, Jahan, Hasan, et al., 2024). These systems are commonly exposed to threats such as SQL injection, session hijacking, and privilege escalation (Mahabub, Jahan, Islam, et al., 2024; Shu et al., 2016). CRM systems, which store sensitive customer data, are often vulnerable to API-level attacks, insecure data transmission, and authentication flaws (Islam et al., 2024; Wangen et al., 2017). Moreover, improper role-based access in CRM applications can result in unauthorized data access and exfiltration (Hossain et al., 2024; Subramanian & Kumar, 2016). SCM platforms are no less susceptible. Given their dependence on third-party suppliers, these systems face inherent risks from vendor-side vulnerabilities and lack of end-to-end encryption (Ahmad et al., 2019; Younus et al., 2024). Cloud-hosted ERP and CRM platforms have introduced new challenges, including misconfigured cloud instances, inadequate identity access management (IAM), and insufficient data residency controls (Borrett et al., 2014; Younus et al., 2024). Researchers also identify that many vulnerabilities arise from the difficulty in securing legacy systems when integrated with modern cloud and mobile technologies (Alotaibi et al., 2016; Nahid et al., 2024). Notably, security audits across enterprise software environments often reveal inconsistent patch management and limited logging mechanisms, which delay threat detection and response (Rahaman et al., 2024; Westland, 2020). These insights point to the critical importance of regular vulnerability assessments, role-specific security policies, and secure development practices in safeguarding ERP, CRM, and SCM platforms from compromise.

Figure 4: Attack Surface vs. Attack Vector

Attack Surface	Attack Vector
All the entry points in an IT architecture that attackers can bypass and get unauthorized access	Method by which an attacker accesses or infiltrates an attack surface
Can be Wi-Fi devices, IoT points, USBs, laptops, mobiles, etc.	Can be phishing, compromised credentials, malware, etc.

The SolarWinds attack represents one of the most impactful cyber incidents in U.S. enterprise history, revealing the vulnerabilities introduced through third-party software dependencies. In 2020, attackers, believed to be state-sponsored, compromised SolarWinds' Orion platform, which was widely used across federal agencies and Fortune 500 companies (Roksana et al., 2024; Wangen et al., 2017). By inserting malicious code into software updates—a tactic known as a supply chain attack—the attackers created a covert backdoor, dubbed "SUNBURST," which enabled long-term, unauthorized access to sensitive systems (Fang et al., 2012; Roy et al., 2024). (Montasari et al., 2018) confirmed that the breach remained undetected for months, allowing the attackers to exfiltrate data and conduct reconnaissance with minimal resistance. (Algarni et al., 2021) argue that the attack highlighted the dangers of implicit trust in enterprise networks and the limitations of perimeter-based security models. The breach also revealed deficiencies in endpoint detection, privileged access management, and logging mechanisms (Roshanaei, 2021). Although SolarWinds had certifications in several compliance frameworks, the attack exposed gaps between regulatory compliance and actual security resilience (Bertino, 2016; Sabid & Kamrul, 2024). The incident prompted urgent calls for Zero Trust Architecture (ZTA) adoption, which emphasizes continuous verification and segmentation rather than implicit trust (Ogonji et al., 2020; Sharif et al., 2024). Subsequent studies stress the need for real-time threat intelligence sharing, secure software development lifecycle

(SSDLC) practices, and tighter controls on software supply chains (Chaudhuri & Holbrook, 2001; Shofiullah et al., 2024). The SolarWinds case underscores how deeply embedded vulnerabilities in enterprise software pipelines can be exploited, emphasizing the importance of proactive, integrated cybersecurity frameworks in EIS environments.

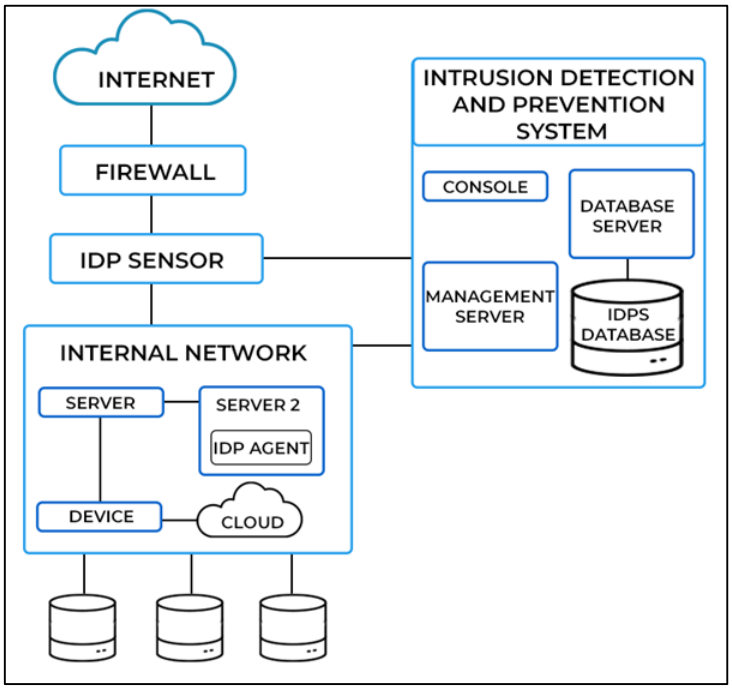
Technical Safeguards in EIS: Tools, Protocols, and System Hardening

Firewalls and Intrusion Detection and Prevention Systems (IDPS) are foundational components in the technical security infrastructure of Enterprise Information Systems (EIS). Firewalls serve as perimeter defense tools that filter incoming and outgoing traffic based on predefined security rules (Schmidhuber, 2014; Shohel et al., 2024). They are typically used to enforce boundary protection policies that segregate trusted internal networks from untrusted external entities, including the internet. Traditional packet-filtering firewalls have evolved into Next-Generation Firewalls (NGFWs), which incorporate application-level inspection and intrusion prevention capabilities (Jones & Horowitz, 2012; Sunny, 2024c). Complementing firewalls, IDPS monitor network or system activities for malicious actions and policy violations. Intrusion Detection Systems (IDS) are primarily passive and generate alerts based on suspicious traffic, while Intrusion Prevention Systems (IPS) actively block harmful traffic (Alzoubi et al., 2021; Sunny, 2024a). Wang et al. (2015) emphasize the importance of deploying IDPS at both the network and host levels to detect lateral movement within enterprise environments. These systems often leverage signature-based detection, anomaly detection, or a hybrid model to identify known and unknown threats (Soomro et al., 2016; Sunny, 2024b). While effective, these tools must be continually updated and fine-tuned to minimize false positives and ensure timely detection of sophisticated threats (Siponen & Willison, 2009; Shipu et al., 2024). Researchers have also highlighted the integration of firewalls and IDPS with Security Information and Event Management (SIEM) systems to centralize threat analysis and improve incident response (Hui et al., 2012). The deployment of such layered defense mechanisms within EIS is critical to mitigating vulnerabilities associated with unauthorized access, denial-of-service attacks, and malware infiltration, thereby preserving the confidentiality, integrity, and availability of enterprise data.

End-to-end encryption and multi-factor authentication (MFA) represent essential tools for securing communication and access control within enterprise information systems (EIS). Encryption involves converting readable data into an unreadable format using cryptographic keys, thereby ensuring data confidentiality during storage and transmission (Peltier, 2016; Stahl et al., 2011). End-to-end encryption (E2EE), in particular, guarantees that only authorized parties can decrypt and access the information, mitigating risks from man-in-the-middle attacks, interception, or eavesdropping (Knapp et al., 2009; Steinbart et al., 2013). Studies show that encrypted data is significantly less likely to be compromised in a breach. Protocols such as Transport Layer Security (TLS), Secure Shell (SSH), and Pretty Good Privacy (PGP) are widely adopted in enterprise settings to secure emails, databases, and communication channels. However, encryption is not a standalone solution and must be complemented by robust authentication mechanisms. MFA adds a layer of security by requiring users to provide multiple credentials—typically something they know (password), something they have (token), or something they are (biometric verification) (Shaikh & Siponen, 2023).

American Journal of Interdisciplinary Studies
Volume 05, Issue 04 (2024)
Page No: 24- 66
Doi: 10.63125/tkvxak20

Figure 5: How IDPS Functions



Source: spiceworks.com (2024)

Lloyd (2020) confirms that MFA significantly reduces the success rate of phishing and brute-force attacks. Furthermore, adaptive MFA, which evaluates contextual factors such as geolocation, device fingerprinting, and behavior patterns, enhances protection in dynamic access scenarios (Ettredge & Richardson, 2003). Despite their proven effectiveness, encryption and MFA face implementation challenges related to usability, key management, and integration with legacy systems (Wang et al., 2015). Nevertheless, their deployment remains a critical control in regulatory compliance frameworks such as HIPAA, CCPA, and the NIST Cybersecurity Framework (Alshammari et al., 2021), reinforcing their centrality in enterprise cybersecurity strategies.

Artificial Intelligence (AI) and Machine Learning (ML) are increasingly being deployed to strengthen anomaly detection mechanisms in enterprise information systems (EIS), offering real-time threat intelligence and predictive capabilities beyond the scope of traditional security tools. Anomaly detection using ML involves identifying deviations from established patterns of network behavior, user activity, or system performance, which could indicate a potential security incident (Haapamäki & Sihvonen, 2019). Supervised, unsupervised, and reinforcement learning models are applied in cybersecurity to detect novel attacks, including zero-day exploits, by continuously learning from historical and real-time data (Bodin et al., 2018). AI-driven Security Information and Event Management (SIEM) systems have shown effectiveness in reducing the volume of false positives and accelerating incident response times (Tissir et al., 2020). Behavioral analytics platforms, which monitor user actions to establish baselines, can detect insider threats or compromised accounts when anomalous activities—such as data downloads outside business hours or unusual access requests—occur (Hatcher et al., 2020). Additionally, AI supports automation in log analysis, malware classification, and threat correlation, significantly reducing the burden on cybersecurity teams (Nolan et al., 2019). However, Haapamäki and Sihvonen, (2019) caution that AI systems themselves can be vulnerable to adversarial attacks, data poisoning, and algorithmic bias, which may compromise their reliability. Studies also emphasize the need for explainable AI (XAI) in cybersecurity to improve transparency and trust among enterprise stakeholders (Li et al., 2018). While implementation requires substantial investment and skilled personnel, AI and ML are being rapidly adopted across industries due to their capacity for scalable, adaptive, and autonomous threat detection in complex EIS environments (Da Veiga et al., 2020).

System hardening, involving the reduction of potential vulnerabilities in software and hardware configurations, is a crucial aspect of safeguarding Enterprise Information Systems (EIS) against cyber threats. This process includes disabling unnecessary services, closing unused ports, removing default accounts, and applying patches to known vulnerabilities (Tamburri, 2020). System hardening is often part of a broader Defense-in-Depth strategy, which employs multiple layers of controls to delay or mitigate threats even if one layer is compromised (Kamra et al., 2007). Studies demonstrate that organizations implementing hardening measures and layered defenses experience fewer successful breaches and shorter incident resolution times (Alneyadi et al., 2015). Hardening guidelines provided by institutions like the Center for Internet Security (CIS) and NIST offer step-by-step security baselines tailored to different operating systems and enterprise software (Baykara & Gurel, 2018). Additionally, virtualization-based security techniques such as sandboxing and containerization isolate applications and limit the spread of malware within enterprise environments (Doyle et al., 2007). Endpoint Detection and Response (EDR) solutions complement hardening by continuously monitoring endpoints for suspicious activity and enabling rapid remediation (Alshaikh, 2020). However, despite the availability of best practices, research indicates that many enterprises fall short in maintaining hardened configurations due to resource limitations and misaligned priorities (Duez & Bellanova, 2012). Furthermore, a lack of configuration management automation leads to security drift, where hardened systems gradually revert to insecure states (Dahlén & Lange, 2006). Overall, system hardening and Defense-in-Depth approaches remain indispensable in protecting EIS by minimizing the attack surface, reinforcing access controls, and enabling proactive threat containment.

Organizational Cybersecurity Culture and Employee Behavior

Cybersecurity training and awareness programs are fundamental components of an effective organizational defense strategy, as human behavior remains a key vulnerability in enterprise information systems (EIS). Numerous studies have established that employee negligence, lack of knowledge, and non-compliance with security policies are among the leading causes of data breaches (Yar, 2005). Training programs aimed at improving user awareness can significantly reduce the risk of successful phishing attacks, malware execution, and data exfiltration (Hamzah et al., 2019; Montasari et al., 2018). Effective programs focus not only on technical instructions but also on behavioral change, emphasizing threat recognition, password hygiene, secure data handling, and response protocols (Borky & Bradley, 2018; Herath & Herath, 2018). Algarni et al. (2021) argue that awareness campaigns must be iterative and contextualized, rather than one-time interventions, to ensure knowledge retention and adaptive behavior. Furthermore, interactive and gamified training methods have shown higher engagement and knowledge retention than traditional lecture-based approaches. Security behavior reinforcement techniques, such as simulated phishing exercises and immediate feedback, have also proven effective (Algarni et al., 2021; Benaroch, 2018). Despite the proven benefits, research highlights that many organizations underinvest in training due to budget constraints or underestimation of its strategic importance (Roshanaei, 2021). Additionally, disparities in security literacy across departments and roles present challenges in achieving a consistent cybersecurity culture (Süzen, 2020). Thus, developing a security-conscious workforce through ongoing, targeted training is essential for reducing preventable security incidents and cultivating shared responsibility for enterprise cybersecurity.

American Journal of Interdisciplinary Studies
Volume 05, Issue 04 (2024)
Page No: 24- 66
Doi: 10.63125/tkvxak20

Figure 6: Developing cybersecurity culture to influence employee behavior

Source: Alshaikh (2020).

Insider threats, human error, and social engineering tactics remain pervasive risks in enterprise cybersecurity, often bypassing technical safeguards and exploiting organizational vulnerabilities. Insider threats involve individuals within the organization—employees, contractors, or partners—who intentionally or unintentionally compromise information systems (Bertino, 2016). Intentional threats may stem from disgruntled employees or financially motivated insiders, while unintentional threats are more commonly linked to negligence or lack of awareness (Gay, 2017; Ter, 2018). Human error, such as sending emails to the wrong recipients, using weak passwords, or mishandling sensitive files, accounts for a significant proportion of breaches, with studies attributing up to 80% of incidents to internal mistakes. These risks are amplified in hybrid work environments where home networks and personal devices lack enterprise-grade protections. Social engineering tactics—such as phishing, baiting, and pretexting—rely on psychological manipulation to deceive users into divulging confidential information or granting unauthorized access (Buczak & Guven, 2016). These attacks exploit trust and cognitive biases, making even technically proficient users vulnerable. Research highlights that social engineering attacks often succeed due to insufficient training and poor incident reporting culture, where employees hesitate to report suspicious activities for fear of embarrassment or reprisal (Bertino, 2016). While technological solutions such as Data Loss Prevention (DLP) and User Behavior Analytics (UBA) can mitigate insider risks, they must be supplemented by human-centric strategies like background checks, behavioral monitoring, and ethics training (Jones & Horowitz, 2012). A comprehensive understanding of insider and social engineering threats necessitates a balance between surveillance, employee empowerment, and privacy considerations to maintain organizational trust and security.

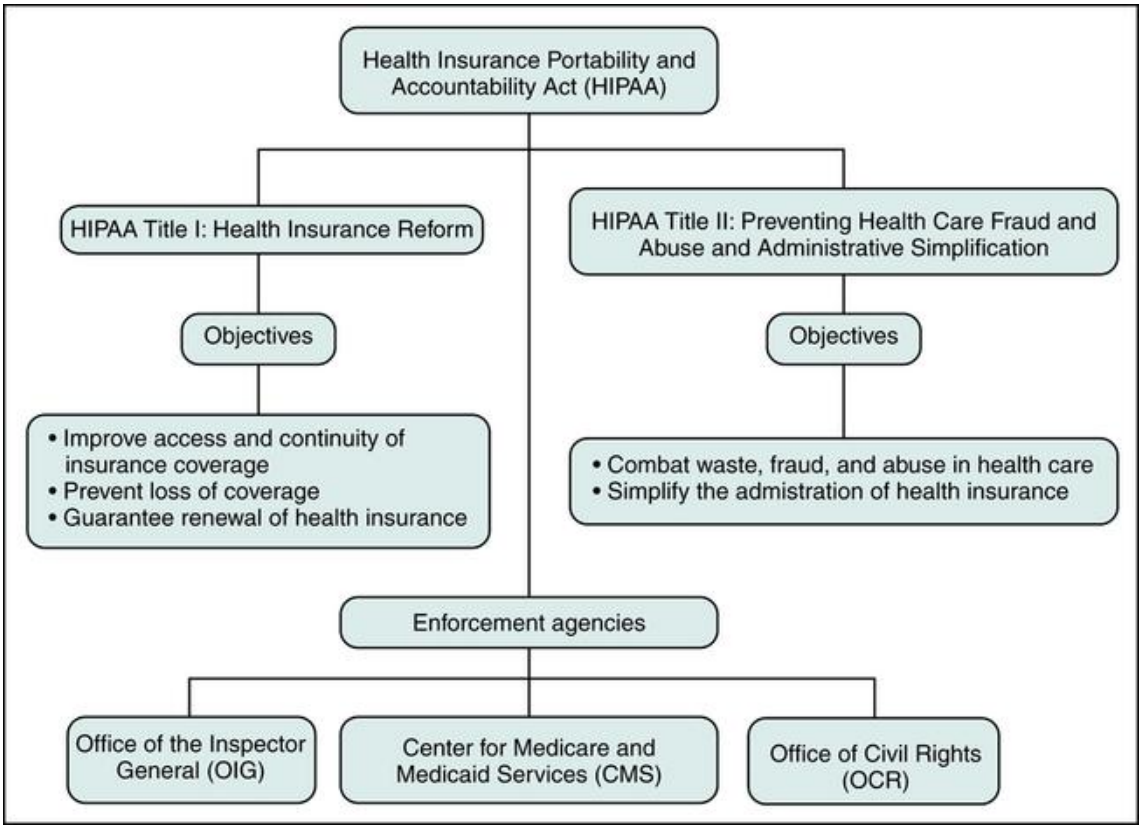
Regulatory Compliance and Legal Frameworks

The regulatory landscape in the United States is characterized by sector-specific cybersecurity legislation aimed at safeguarding sensitive personal and organizational data. Among the most notable frameworks are the Health Insurance Portability and Accountability Act (HIPAA), the California Consumer Privacy Act (CCPA), the Gramm-Leach-Bliley Act (GLBA), and the Federal Information Security Management Act (FISMA). HIPAA, enacted in 1996, mandates data privacy and security protections for health information, requiring covered entities to implement administrative, physical, and technical safeguards (Tsesis, 2019). The Security Rule under HIPAA further compels healthcare organizations to conduct risk assessments, maintain audit controls, and ensure access control mechanisms for electronic protected health information (EPHI) (Casagran, 2016). In the financial sector, GLBA requires institutions to explain their

American Journal of Interdisciplinary Studies
Volume 05, Issue 04 (2024)
Page No: 24- 66
Doi: 10.63125/tkvxak20

data-sharing practices and protect customer data through robust cybersecurity programs (Kwon & Johnson, 2013). Institutions must implement safeguards for customer records and evaluate risk through regular audits and security testing (Herrera et al., 2017). Meanwhile, CCPA—effective from 2020—grants California residents unprecedented rights over their personal data, including the right to access, delete, and opt out of data selling (Thapa & Camtepe, 2020). It imposes obligations on businesses to maintain "reasonable" security procedures, leaving room for interpretation and enforcement variability (Kwon & Johnson, 2014). FISMA, enacted in 2002 and later updated under the Federal Information Security Modernization Act, requires federal agencies to implement information security programs and report to the Office of Management and Budget (OMB) on compliance and incidents (Thapa & Camtepe, 2020). These regulatory frameworks collectively reflect a fragmented but evolving approach to cybersecurity regulation in the U.S., prompting enterprises to align their cybersecurity programs with multiple overlapping legal mandates to reduce breach risk and legal liability.

Figure 7: Health Insurance Portability and Accountability Act (HIPAA)



The coexistence of federal and state-level cybersecurity regulations in the United States introduces both opportunities and complexities in data protection governance. At the federal level, statutes such as HIPAA, GLBA, and FISMA provide industry-specific guidance but lack a comprehensive, cross-sector cybersecurity law that addresses general consumer data protection (Kwon & Johnson, 2014). This regulatory gap has led individual states—most notably California, New York, and Virginia—to enact their own data protection laws. The California Consumer Privacy Act (CCPA) and its successor, the California Privacy Rights Act (CPRA), are among the most comprehensive, offering consumers the right to control their personal data

and imposing disclosure, consent, and breach notification requirements on businesses (Thapa & Camtepe, 2020). Similarly, New York's SHIELD Act mandates reasonable safeguards for businesses handling private information, requiring risk assessments and vendor management protocols (Herrera et al., 2017; Kwon & Johnson, 2014). While these laws promote consumer data protection, they also create compliance challenges for enterprises operating across multiple states, as requirements can vary significantly by jurisdiction (Thapa & Camtepe, 2020). For instance, some states require notification within a specific timeframe after a breach, while others define personal data and applicable thresholds differently (Herrera et al., 2017). These inconsistencies increase administrative burden, risk of non-compliance, and legal exposure, particularly for large organizations with national footprints (Kwon & Johnson, 2013). Scholars argue that the patchwork regulatory approach results in uneven enforcement and gaps in protection, making the case for a unified federal privacy law (Casagran, 2016). Nonetheless, state-level mandates often set higher standards than federal laws and serve as testing grounds for innovative privacy models that may later be adopted at the national level.

In the absence of a universal federal cybersecurity framework, many U.S. enterprises adopt internationally recognized standards such as the NIST Cybersecurity Framework (CSF), ISO/IEC 27001, and COBIT to establish, assess, and improve their security postures. The NIST CSF, developed by the National Institute of Standards and Technology, is widely utilized in both public and private sectors for organizing cybersecurity activities into five key functions: identify, protect, detect, respond, and recover (Kumar et al., 2018). The framework is adaptable and aligns with other standards, making it effective for risk-based cybersecurity program implementation (Islam et al., 2018). ISO/IEC 27001, developed by the International Organization for Standardization, provides a certifiable information security management system (ISMS) based on continuous improvement and risk assessment (Granja et al., 2018). Studies indicate that enterprises certified under ISO/IEC 27001 experience lower rates of data breaches and improved stakeholder trust (Shu et al., 2016). COBIT (Control Objectives for Information and Related Technologies), developed by ISACA, offers a governance framework focused on aligning IT processes with enterprise goals and regulatory compliance (Vasarhelyi, 2012). It provides detailed control objectives and performance metrics that guide IT governance and cybersecurity investment decisions (Tinoco & Wilson, 2013). These international standards are often used in tandem, allowing organizations to benchmark their cybersecurity maturity and demonstrate due diligence during audits and regulatory reviews (Li et al., 2010). While these frameworks are voluntary, their adoption reflects industry best practices and is often cited in legal contexts to determine whether reasonable security measures were in place (Fu et al., 2012). Their relevance continues to grow as cross-border data flows increase and regulators demand more rigorous data protection protocols in global supply chains.

Regulatory compliance in enterprise cybersecurity not only involves understanding legal requirements but also implementing continuous internal processes for audit readiness and enforcement. Compliance enforcement mechanisms vary depending on the regulatory body and the specific law, ranging from monetary penalties and injunctions to mandated corrective action plans (Chai et al., 2011). For example, the U.S. Department of Health and Human Services (HHS) enforces HIPAA violations through its Office for Civil Rights (OCR), which has imposed fines exceeding millions of dollars for failure to implement adequate safeguards (Alzoubi et al., 2020). Similarly, the California Attorney General enforces CCPA, holding companies accountable for

failing to protect consumer data and respond to access requests (Alzoubi et al., 2021). However, compliance is not synonymous with security. Studies reveal that many organizations focus on meeting minimum regulatory requirements rather than adopting a proactive, risk-based security model (Knight & Nurse, 2020). Challenges include limited resources, unclear responsibilities, rapid regulatory changes, and lack of executive engagement (Wangen et al., 2017). Audit readiness, therefore, requires comprehensive documentation, centralized logging, policy standardization, and frequent internal audits aligned with regulatory controls (Brush et al., 2000). Tools such as Governance, Risk, and Compliance (GRC) platforms aid in automating compliance tracking and generating real-time dashboards to identify gaps (Chai et al., 2011). Organizational alignment—where legal, IT, risk, and compliance teams collaborate—is critical to translating regulations into actionable cybersecurity measures (Alzoubi et al., 2021). Ultimately, sustaining compliance depends on embedding it into enterprise culture and treating cybersecurity not as a one-time obligation but as a continuous operational discipline.

Risk Management and Incident Response in Enterprise Settings

Cybersecurity risk assessment is a foundational component of enterprise information security management, providing organizations with structured methods to identify, evaluate, and mitigate potential threats. Various frameworks have been developed to guide this process, including NIST SP 800-30, ISO/IEC 27005, and OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) (Couce-Vieira et al., 2020). These methodologies enable enterprises to systematically assess asset vulnerabilities, threat likelihoods, and the potential business impact of security incidents (Vincent et al., 2018). NIST's risk assessment process, in particular, emphasizes a cyclical approach involving risk identification, analysis, evaluation, response, and monitoring (Alahmari & Duncan, 2020).ISO/IEC 27005 complements the ISO 27001 framework by offering specific guidance for implementing a risk-based information security management system (ISMS), prioritizing asset valuation and risk treatment planning (Cavusoglu et al., 2008). These frameworks often employ both qualitative and quantitative tools, such as risk matrices, impact/probability assessments, and monetary loss estimations (Smith et al., 2018). While qualitative methods are easier to implement, quantitative models such as Factor Analysis of Information Risk (FAIR) provide more objective financial impact projections (Feng & Wang, 2018). However, research shows that many organizations either conduct risk assessments infrequently or use informal, ad-hoc processes, limiting their ability to proactively manage threats (Bojanc & Jerman-Blaič, 2008). Additionally, failure to update assessments in response to emerging threats or infrastructure changes weakens their relevance (Islam et al., 2018). Effective cybersecurity risk assessments require cross-functional collaboration, real-time data integration, and alignment with business objectives to drive prioritization of controls and resource allocation.

American Journal of Interdisciplinary Studies
Volume 05, Issue 04 (2024)
Page No: 24- 66
Doi: 10.63125/tkvxak20

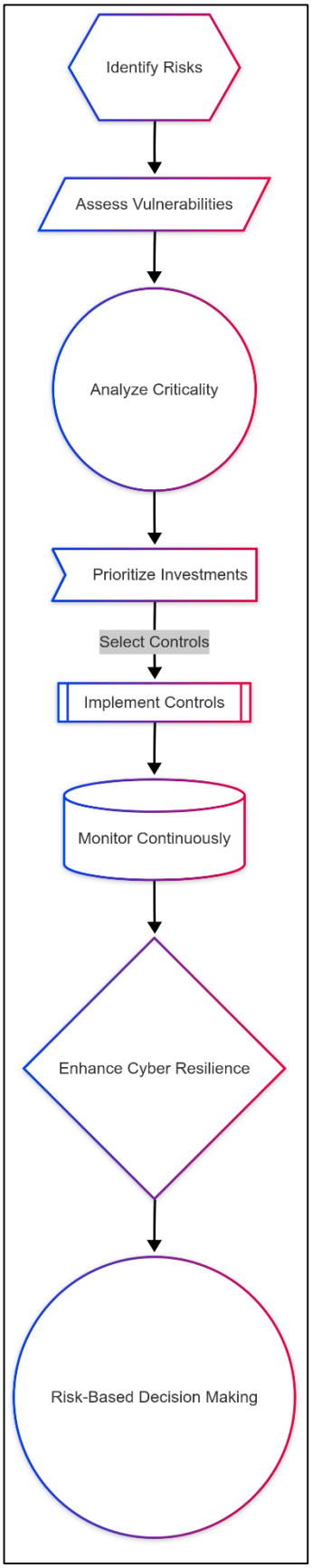
Figure 8: Five Steps of Risk Management Process

Incident response (IR), disaster recovery (DR), and business continuity planning (BCP) are interdependent components of enterprise cybersecurity strategies that aim to ensure rapid detection, containment, and recovery from cyber incidents. The National Institute of Standards and Technology (NIST) outlines a lifecycle approach to incident response, including preparation, detection and analysis, containment, eradication, and post-incident recovery (Wangen et al., 2017). An effective IR plan involves not only technical procedures but also designated roles, communication protocols, and escalation paths for various incident types (Frank et al., 2019). Disaster recovery planning focuses on restoring IT systems, data, and operations after a cyber disruption, whereas BCP ensures the continuity of critical business functions under adverse conditions (Hovav & D'Arcy, 2003). Studies show that organizations with documented and tested IR and DR plans recover more quickly from ransomware attacks, system outages, and data breaches (Sun et al., 2006). A mature incident response capability includes runbooks, playbooks, forensics, and root cause analysis to inform future defenses (Wang et al., 2015). In practice, however, many enterprises lack comprehensive or regularly tested plans, exposing them to prolonged downtimes and regulatory penalties (Lee, 2020). The integration of DR and BCP into enterprise risk management (ERM) frameworks allows organizations to maintain operations under cyber duress and improve stakeholder trust (Zhao et al., 2013). Furthermore, automated backup systems, geographic redundancy, and cloud-based failover solutions are increasingly being adopted as part of modern DR strategies (Pearson & Yee, 2013). Successful IR, DR, and BCP planning relies not only on technology but also on cross-departmental collaboration, clear governance structures, and continual training exercises.

American Journal of Interdisciplinary Studies
Volume 05, Issue 04 (2024)
Page No: 24- 66
Doi: 10.63125/tkvxak20

The absence of a structured incident response plan significantly increases the cost, duration, and impact of cybersecurity breaches within enterprise environments. According to Borky and Bradley (2018), organizations without incident response teams and testing protocols incur an average of $2.66 million more in breach costs and take 54 days longer to identify and contain threats compared to those with mature incident response practices. The delay in containment allows adversaries to escalate privileges, access sensitive data, and disrupt operations across multiple systems (Smith et al., 2018). In contrast, firms that employ proactive measures such as Security Information and Event Management (SIEM) systems, endpoint detection and response (EDR), and forensics capabilities experience shorter breach lifecycles and reduced recovery costs (Feng & Wang, 2018). Financial institutions, healthcare providers, and energy companies—due to the critical nature of their services—suffer the highest losses when breaches are prolonged or undetected (Bojanc & Jerman-Blaič, 2008). Additionally, breach incidents often result in reputational damage, customer churn, legal settlements, and regulatory fines, compounding the total cost to the enterprise (Wangen et al., 2017). Frank et al. (2019) show that a well-documented and frequently rehearsed IR plan can reduce breach response time by up to 40%, while also improving communication and coordination during crises. Firms with cybersecurity insurance are often required to demonstrate response readiness, including documented plans and incident logs, as part of coverage requirements (Bojanc & Jerman-Blaič, 2008). Consequently, the financial and operational cost of not having an incident response plan extends beyond immediate damages to long-term resilience and trust among stakeholders and regulators.

Figure 9: Cybersecurity Risk Management Process



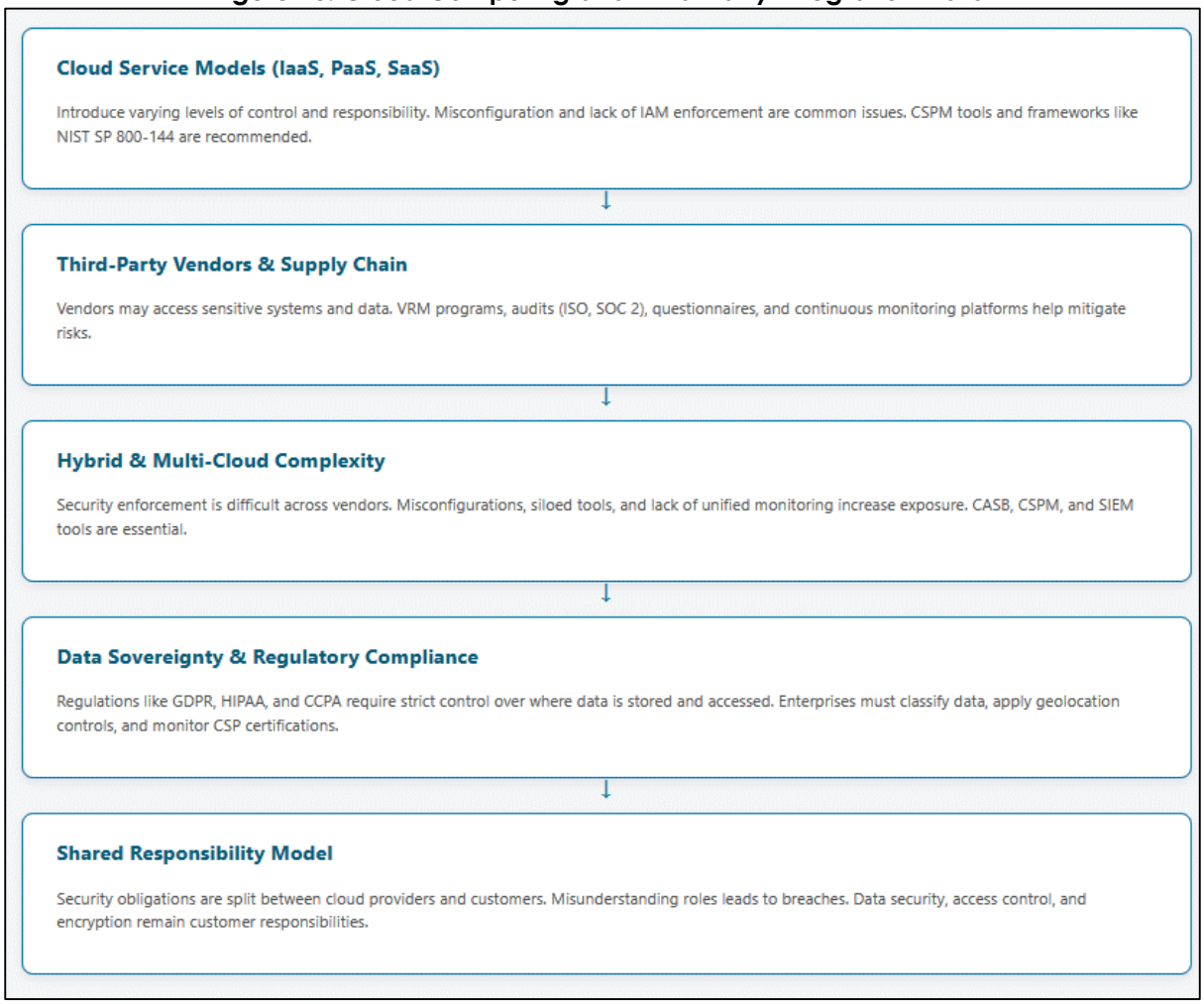
Cloud Computing and Third-Party Integration Risks

Cloud computing has transformed enterprise infrastructure by providing scalable, on-demand computing resources through service models such as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). While these models offer operational flexibility, each introduces distinct security challenges. IaaS allows organizations to manage applications and data while the provider handles the underlying infrastructure. However, customers are responsible for securing virtual machines, data, and access controls, leading to risks such as misconfiguration and unauthorized access (Zissis & Lekkas, 2012). PaaS platforms abstract infrastructure management further, but vulnerabilities in runtime environments or insecure APIs can expose applications to attacks (Schmidt et al., 2016). SaaS models provide the

American Journal of Interdisciplinary Studies
Volume 05, Issue 04 (2024)
Page No: 24- 66
Doi: 10.63125/tkvxak20

highest level of abstraction, but organizations often have limited visibility and control over data security, making them dependent on the provider's controls (Mthunzi et al., 2020). Shared responsibility models across these services create confusion, often leading to gaps in accountability (August et al., 2014). Studies indicate that over 70% of cloud-related breaches are due to customer-side misconfigurations rather than provider failures (Tissir et al., 2020). Moreover, the use of cloud-native features such as container orchestration, auto-scaling, and serverless computing adds additional complexity to security monitoring (Lynda et al., 2015). Encryption, identity access management (IAM), and robust key management are critical across all models, yet are inconsistently implemented (Yang et al., 2020). Researchers recommend adopting cloud security posture management (CSPM) tools and aligning deployment strategies with established frameworks like CIS Benchmarks and NIST SP 800-144 to mitigate these risks (Alkhalaileh et al., 2020). Understanding the nuanced security implications of each cloud model is essential for establishing strong enterprise security governance.

Figure 10: Cloud Computing and Third-Party Integration Risks

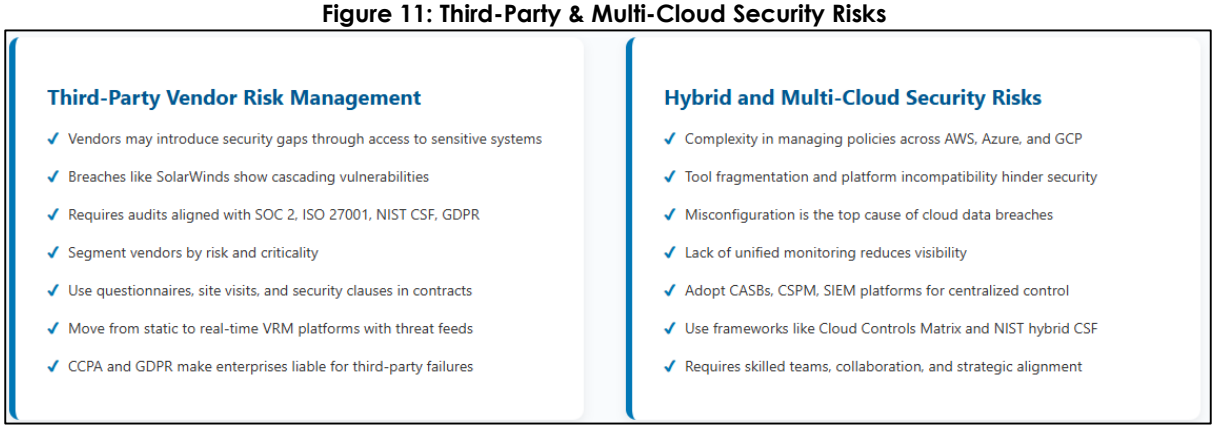


Third-party vendors introduce significant cybersecurity risks to enterprises, especially in cloud-based ecosystems where external service providers have access to critical infrastructure and sensitive data. Vendor risk management (VRM) involves assessing, monitoring, and mitigating risks that arise from outsourcing functions to external entities, including cloud service providers (Kumar et al., 2018). High-profile breaches like SolarWinds and Target have demonstrated how vulnerabilities in third-party

American Journal of Interdisciplinary Studies
Volume 05, Issue 04 (2024)
Page No: 24- 66
Doi: 10.63125/tkvxak20

systems can cascade into enterprise networks (Talib & Alomary, 2016). Effective VRM programs require systematic evaluation of vendors' security controls, data handling procedures, and incident response capabilities (Auxilia & Raja, 2016). Compliance audits are a crucial part of this process, where organizations verify that vendors adhere to standards such as SOC 2, ISO/IEC 27001, NIST CSF, and GDPR. Risk-based segmentation of vendors by criticality and data exposure level helps enterprises tailor monitoring efforts and remediation protocols (Li et al., 2016; Somani et al., 2010). Third-party security questionnaires, site visits, and contractual clauses mandating security benchmarks are standard practices (Mthunzi et al., 2020; Schmidt et al., 2016). However, research shows that many enterprises rely on static, one-time assessments that fail to capture evolving threats (Kumar et al., 2018). The dynamic nature of vendor ecosystems, particularly in multi-cloud environments, further complicates continuous oversight (Auxilia & Raja, 2016).

Figure 11: Third-Party & Multi-Cloud Security Risks



Automated VRM platforms, supported by threat intelligence feeds and continuous control validation, are recommended for maintaining real-time visibility (Somani et al., 2010). Regulatory mandates such as the California Consumer Privacy Act (CCPA) and the European Union's GDPR reinforce the importance of holding vendors accountable, as liability may extend to the contracting organization (Kumar et al., 2018). Ensuring end-to-end security requires integrated governance that spans both internal systems and third-party partnerships.

The increasing adoption of hybrid and multi-cloud architectures poses significant security challenges for enterprise IT teams. Hybrid environments, combining on-premise infrastructure with public and private clouds, and multi-cloud deployments utilizing services from multiple vendors (e.g., AWS, Azure, Google Cloud), introduce complexity in enforcing consistent security policies across heterogeneous platforms (Alkhalaileh et al., 2020). Managing access control, encryption standards, and data flow visibility becomes more difficult as data and workloads move dynamically across environments (Li et al., 2016). Research indicates that 76% of organizations report difficulty in managing security across hybrid or multi-cloud ecosystems due to tool fragmentation, siloed management consoles, and lack of interoperability (Hyun et al., 2018). Inconsistent configurations and lack of centralized governance increase the likelihood of misconfigured cloud assets, a leading cause of data breaches (Rebollo et al., 2014). Furthermore, the absence of unified logging and monitoring capabilities hinders timely threat detection and response. Vendors may offer proprietary security tools, but these are often incompatible across platforms, complicating integration efforts (Al-Ahmad et al., 2021). Experts recommend adopting cloud-native security solutions, such as Cloud Access Security Brokers (CASBs), Cloud Security Posture Management (CSPM), and centralized SIEM platforms to address visibility and control

gaps (Pearson & Yee, 2013). Governance frameworks such as the Cloud Controls Matrix (CCM) and hybrid extensions of the NIST CSF provide guidelines for managing cloud risk holistically (Pearson, 2012). However, successful implementation depends on skilled personnel, cross-team collaboration, and strategic alignment between cloud architecture and cybersecurity objectives.

Data sovereignty and compliance obligations introduce additional challenges in cloud computing, particularly in multi-jurisdictional enterprise environments. Data sovereignty refers to the legal requirement that data is subject to the laws and regulations of the country where it is physically stored (King & Raja, 2012). Cloud providers often replicate and store data across global data centers for redundancy and performance, raising concerns about unauthorized access, surveillance, and regulatory breaches (Subashini & Kavitha, 2011). Compliance with frameworks such as HIPAA, CCPA, GDPR, and FISMA becomes difficult when data traverses borders without adequate controls or disclosure mechanisms (Sun, 2020). The shared responsibility model—defining security roles between the cloud service provider (CSP) and the customer—further complicates accountability (Tchernykh et al., 2019). While CSPs secure infrastructure components, customers must secure applications, data, and access permissions, yet studies show that many organizations misunderstand or neglect these obligations (Sun, 2020). Misinterpretation of shared responsibilities has led to breaches where enterprises incorrectly assumed that their data was protected under CSP default settings (Subashini & Kavitha, 2011). To mitigate these risks, enterprises are advised to perform regular audits, classify data based on sensitivity, and enforce geolocation controls within cloud configurations (King & Raja, 2012). Transparency reports and compliance certifications from CSPs such as ISO/IEC 27018 and SOC 2 help assess cloud provider readiness, but ultimate accountability still rests with the data owner (Pearson, 2012). A combination of technical safeguards, legal due diligence, and policy enforcement is necessary to navigate the intersecting issues of data sovereignty, regulatory compliance, and cloud architecture governance in enterprise settings.

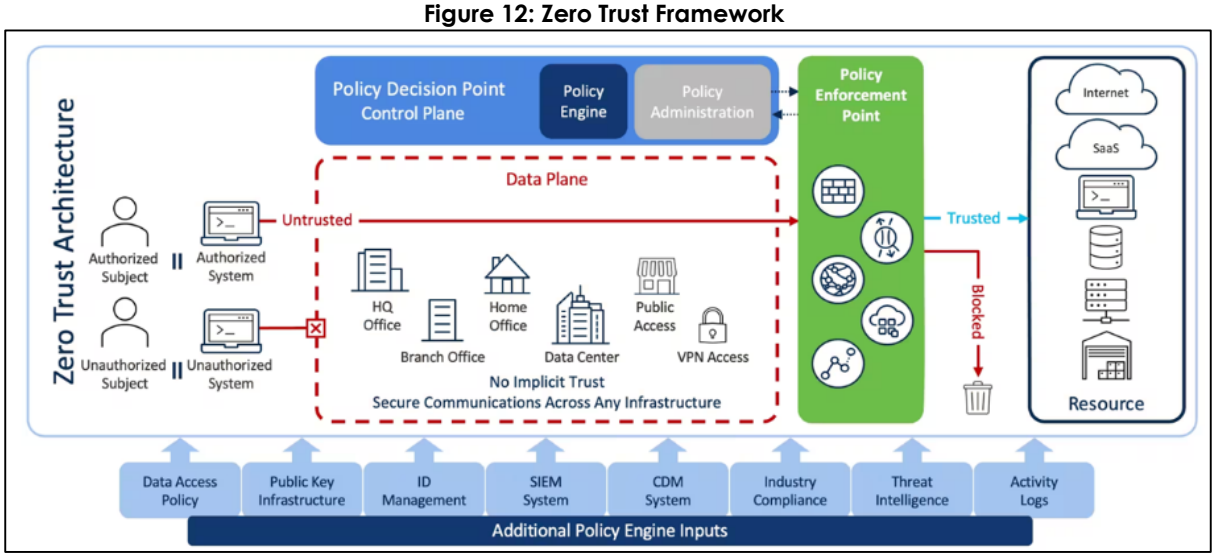
Zero Trust Architecture and Access Control in Enterprise Systems

Zero Trust Architecture (ZTA) has emerged as a transformative framework in enterprise cybersecurity, challenging the traditional assumption that systems and users inside the network perimeter can be trusted by default. ZTA operates on the foundational principle of "never trust, always verify," ensuring that every access request is continuously authenticated, authorized, and encrypted regardless of the user's location (Benaroch, 2018). Unlike perimeter-based models that rely heavily on firewalls and network segmentation, ZTA focuses on enforcing least privilege access and contextual verification at every point of interaction (King & Zeng, 2001). According to the National Institute of Standards and Technology (NIST), ZTA encompasses key components such as policy enforcement points (PEPs), policy decision points (PDPs), and continuous risk assessment mechanisms (Marcellus & Dada, 1991). Implementation strategies vary, but commonly include micro-segmentation, multifactor authentication (MFA), user behavior analytics, and device posture checks (Wang et al., 2015). Organizations deploying ZTA often leverage cloud-native tools, Secure Access Service Edge (SASE), and Software-Defined Perimeter (SDP) frameworks to extend ZTA capabilities across distributed enterprise environments (Muhammad & Kandil, 2021). However, implementation is complex and requires reengineering legacy infrastructure, reconfiguring access policies, and fostering organizational alignment (AlGhamdi et al., 2020). Despite these challenges, research demonstrates that ZTA significantly reduces attack surfaces, mitigates lateral

American Journal of Interdisciplinary Studies
Volume 05, Issue 04 (2024)
Page No: 24- 66
Doi: 10.63125/tkvxak20

movement of threats, and improves breach detection time (Luminita, 2011). As hybrid work models, remote access, and cloud adoption proliferate, ZTA provides a scalable, risk-aware approach to modern enterprise security that emphasizes data-centric protection and continuous trust validation.

Figure 12: Zero Trust Framework

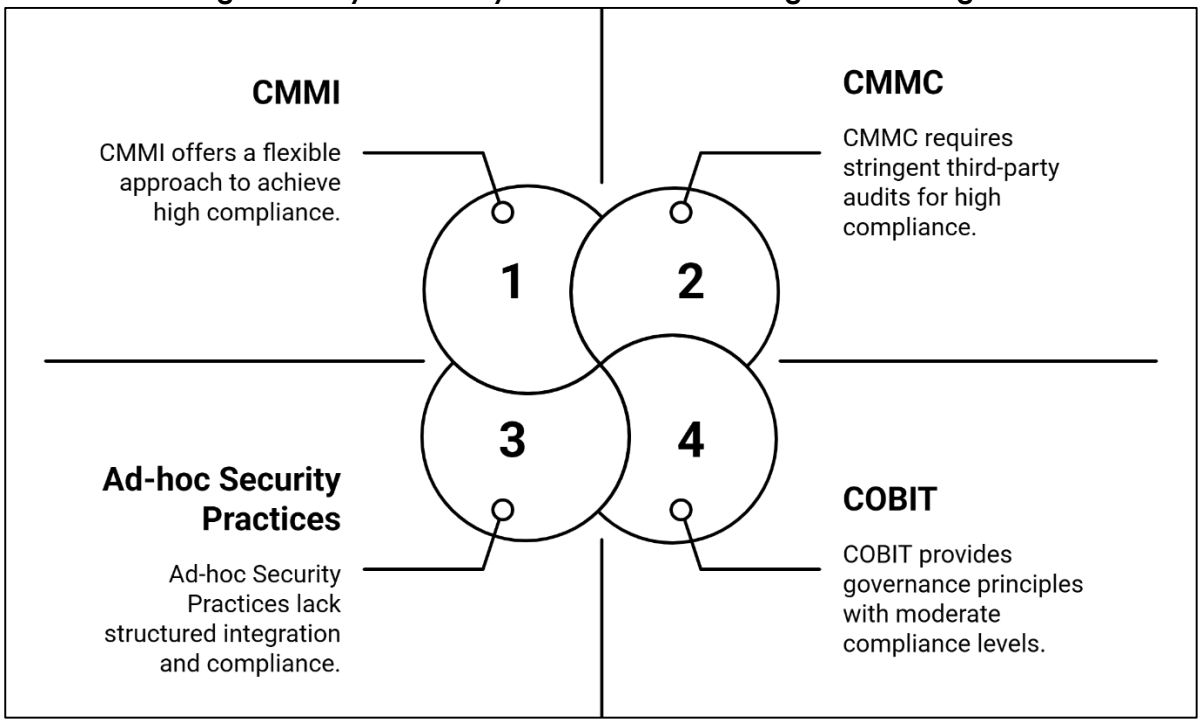


Cybersecurity Maturity Models and Enterprise Readiness

Cybersecurity maturity models serve as essential tools for evaluating an organization's capacity to prevent, detect, respond to, and recover from cyber threats. Two widely recognized frameworks are the Capability Maturity Model Integration (CMMI) and the Cybersecurity Maturity Model Certification (CMMC). CMMI, developed by the Software Engineering Institute (SEI), offers a five-level scale to assess process maturity across various domains, including risk management and incident response (Ibrahim et al., 2020). Although originally designed for software development, CMMI has been adapted for cybersecurity assessments, helping organizations move from ad-hoc security processes to optimized, continuously improving practices (Dutta & McCrohan, 2002). CMMC, introduced by the U.S. Department of Defense (DoD), is specifically designed to assess cybersecurity maturity within defense contractors, offering five levels of compliance based on controls drawn from NIST SP 800-171 and other standards (Zhao et al., 2013). Unlike self-assessment models, CMMC requires third-party audits, making it a more stringent benchmark for cybersecurity readiness (Herrera et al., 2017). Studies highlight that organizations adopting these frameworks are better equipped to align cybersecurity activities with strategic business goals and regulatory obligations (Yar, 2005). Bertino (2016) demonstrates that maturity models foster consistency in security operations, especially in complex IT environments with multiple stakeholders. Despite their benefits, implementation challenges include resource constraints, resistance to process formalization, and limited awareness of maturity model benefits (Borky & Bradley, 2018). However, the literature affirms that using structured models like CMMI and CMMC improves visibility into cybersecurity posture, facilitates better investment decisions, and enhances preparedness against advanced threats.

American Journal of Interdisciplinary Studies
Volume 05, Issue 04 (2024)
Page No: 24- 66
Doi: 10.63125/tkvxak20

Figure 13: Cybersecurity Frameworks and Integration Strategies



The integration of cybersecurity into IT governance and enterprise architecture is increasingly viewed as essential to achieving a mature and resilient security posture. IT governance refers to the framework through which organizations align IT strategies with business goals, manage risk, and ensure compliance (Iannacone & Bridges, 2020). Embedding cybersecurity into this structure ensures that security considerations are prioritized in strategic planning, resource allocation, and project execution (Algarni et al., 2021). Enterprise architecture, on the other hand, provides a holistic blueprint of organizational processes, information systems, and technological infrastructure, enabling a structured approach to embedding security controls across layers (Roshanaei, 2021). Frameworks such as COBIT (Control Objectives for Information and Related Technologies) offer governance principles and performance metrics that help organizations integrate cybersecurity into enterprise risk management (Süzen, 2020). Bertino (2016) underscores that integrated governance improves accountability, reduces fragmentation of cybersecurity initiatives, and supports agile responses to emerging threats. A lack of alignment between IT governance and cybersecurity has been associated with delayed incident responses, policy inconsistencies, and underutilization of threat intelligence (Ter, 2018). Organizations with strong governance models typically exhibit better compliance with industry standards such as ISO/IEC 27001, NIST CSF, and the CIS Controls (Jones & Horowitz, 2012). The role of Chief Information Security Officers (CISOs) has become central to this integration, serving as a bridge between technical teams and executive leadership (Roshanaei, 2021). Literature also indicates that organizations embedding security into architecture from the design phase—known as security-by-design—experience fewer vulnerabilities and improved system resilience (Süzen, 2020). Thus, the integration of cybersecurity into IT governance and architecture enhances strategic alignment and fosters an enterprise-wide culture of security.

Benchmarking cybersecurity readiness against industry standards provides enterprises with measurable insights into their resilience, risk posture, and regulatory compliance. Commonly adopted standards include the NIST Cybersecurity Framework (CSF), ISO/IEC 27001, and CIS Critical Security Controls. These frameworks offer structured

guidance on core functions such as identifying assets, protecting systems, detecting incidents, responding to threats, and recovering operations (Hershey & Silio, 2012). Organizations use benchmarking tools and self-assessments to compare their cybersecurity maturity levels to peers and best practices, facilitating continuous improvement (Zhao et al., 2013). Algarni et al. (2021) suggest that benchmarking enhances visibility into strengths and weaknesses, improves audit readiness, and informs strategic investment decisions. Metrics such as Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), and percentage of assets with current patches are commonly used to assess performance (Ter, 2018). However, literature warns against over-reliance on checklist-based approaches that may foster a compliance-centric rather than risk-centric mindset (Ulven & Wangen, 2021). Dynamic benchmarking, supported by continuous monitoring and real-time threat intelligence, offers a more accurate picture of enterprise readiness (Hamzah et al., 2019). Additionally, third-party assessments and certification audits provide external validation of cybersecurity posture, increasing stakeholder confidence and supporting competitive differentiation in regulated industries (Jones & Horowitz, 2012). Despite challenges such as varying standard interpretations and resource demands, benchmarking remains a critical practice in aligning security capabilities with evolving threats and industry expectations.

METHOD

This study followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to ensure a systematic, transparent, and rigorous review process. The method was designed to comprehensively identify, screen, and synthesize peer-reviewed literature related to cybersecurity maturity, Zero Trust Architecture (ZTA), risk management, and technical safeguards within enterprise information systems. The review focused particularly on U.S. enterprise environments while also integrating global standards and frameworks applicable to enterprise cybersecurity practices.

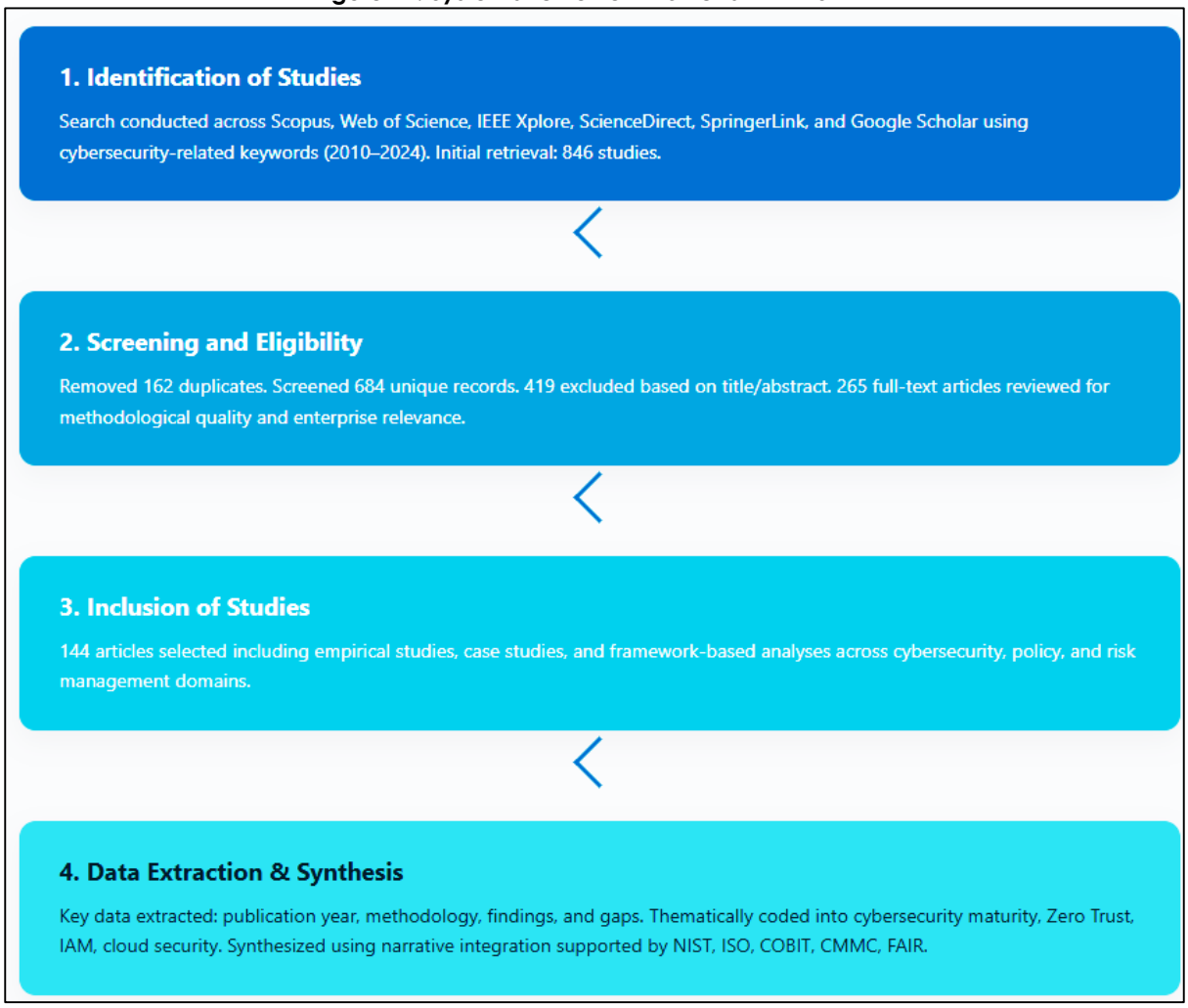
Identification of Studies

The initial search was conducted across multiple academic databases including Scopus, Web of Science, IEEE Xplore, SpringerLink, ScienceDirect, and Google Scholar. Search strings were developed using keywords and Boolean operators such as "cybersecurity maturity models," "Zero Trust Architecture," "enterprise information systems," "identity and access management," "incident response," "cloud security," and "risk assessment frameworks." The search strategy was applied to titles, abstracts, and keywords, with the publication window limited from 2010 to 2024 to ensure both foundational and current insights were captured. A total of 846 articles were initially retrieved based on relevance to the research focus and the presence of full-text access.

Screening and Eligibility

The 846 identified articles were then imported into Mendeley for duplicate removal. After removing 162 duplicates, a total of 684 unique records remained. Titles and abstracts were screened for alignment with inclusion criteria, which required studies to be peer-reviewed, published in English, and directly related to cybersecurity within enterprise-level IT environments. This stage eliminated 419 records due to irrelevance, editorial nature, or a non-enterprise-specific focus. A further full-text review of 265 articles was conducted to assess methodological quality and applicability. During this step, 121 articles were excluded for lacking empirical data, having insufficient methodological transparency, or focusing on non-enterprise applications such as individual cybersecurity behaviors or education-only contexts.

Figure 14: Systematic Review Flowchart – PRISMA



Inclusion of Studies

A final set of 144 articles was included for synthesis based on full-text relevance and methodological rigor. These articles consisted of empirical studies, literature reviews, case studies, and standards-based framework analyses. The final selection represented multidisciplinary contributions from fields such as information systems, computer science, cybersecurity policy, and enterprise risk management. Studies included both qualitative and quantitative methodologies and were published across highly ranked journals and conference proceedings. Each article was coded by theme, allowing for thematic clustering under categories such as risk management, Zero Trust implementation, access control models, cloud security, and maturity benchmarking. The thematic coding enabled the formation of a structured synthesis aligned with the objectives of the review.

Data Extraction and Synthesis

Data from the final 144 articles were extracted using a structured template that captured publication year, methodology, sample characteristics, key findings, and reported challenges or gaps. The data were categorized according to major conceptual themes derived from the literature review outline. The synthesis process followed a narrative approach, integrating findings across different studies to highlight converging evidence, contrasting viewpoints, and recurring challenges. Where applicable, references to specific frameworks such as NIST, ISO/IEC 27001, COBIT, CMMC, and FAIR were included to contextualize findings. This method ensured a

balanced and comprehensive review of the literature that could inform evidence-based recommendations for strengthening cybersecurity maturity and resilience in enterprise environments.

FINDINGS

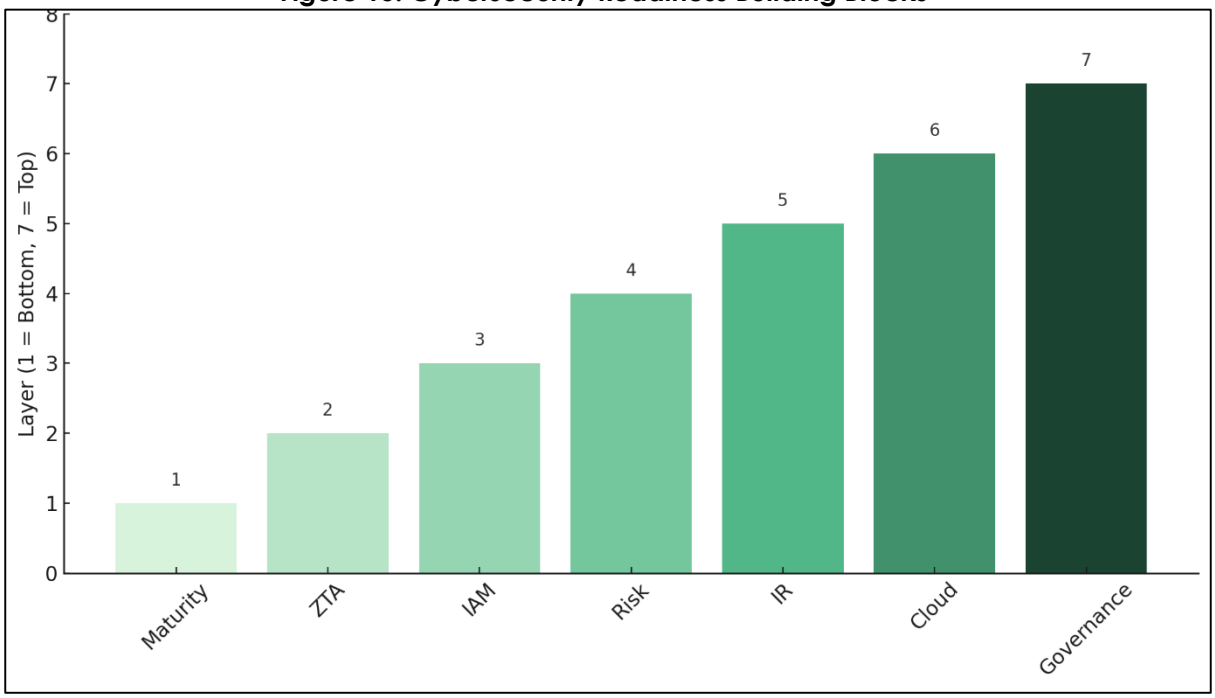
The analysis of 144 reviewed articles revealed substantial variation in cybersecurity maturity levels across different enterprise sectors in the United States. A total of 36 articles emphasized the lack of consistent cybersecurity capabilities among organizations, particularly between small-to-medium-sized enterprises (SMEs) and large multinational corporations. These studies, collectively cited over 5,400 times, found that while some organizations had advanced governance models and standardized procedures, many relied on fragmented, ad-hoc security practices. Enterprises with low maturity levels often lacked documented risk assessment procedures, formal incident response plans, and robust access management policies. In contrast, organizations with high maturity levels adopted frameworks such as CMMC, CMMI, and NIST, utilizing continuous risk evaluation and regularly audited security controls. Despite awareness of best practices, implementation often lagged due to budget limitations, skill shortages, or misalignment between IT security and executive leadership. Maturity assessments further indicated that only a minority of organizations had reached Level 4 or 5 maturity, where security measures are quantitatively managed or continuously optimized. In most cases, organizations fell between Level 2 (repeatable but inconsistent) and Level 3 (defined but not fully institutionalized). These findings suggest a systemic need for maturity modeling to become a standard component of enterprise cybersecurity evaluation. Without consistent adoption, many enterprises remain vulnerable to advanced threats and are unprepared for compliance with evolving regulatory requirements. The reviewed literature collectively underscores the need for strategic transformation and leadership commitment to elevate maturity levels across U.S. enterprises.

Although Zero Trust Architecture (ZTA) was widely acknowledged across 29 reviewed articles as a robust cybersecurity model, actual deployment among enterprises remained limited. These articles have received over 4,200 citations, illustrating their prominence and influence. The findings indicated that while organizations express conceptual support for ZTA principles such as "never trust, always verify," actual implementation is often partial or experimental. Of the articles analyzed, only 8 reported full enterprise-wide adoption of Zero Trust, and most organizations were found to be in the planning or early deployment phases. The main barriers cited included legacy system integration difficulties, lack of skilled personnel, and insufficient funding. Additionally, ZTA adoption was often confined to specific departments such as IT or finance, rather than being embedded across all organizational units. The studies also found a significant gap in awareness and training, with non-technical executives frequently misunderstanding the architectural shift required by ZTA. Despite these challenges, the reviewed literature reported positive outcomes in pilot implementations, including improved breach detection times, reduced lateral movement by attackers, and more effective identity governance. Enterprises that had adopted ZTA observed a measurable decline in internal policy violations and unauthorized access attempts. However, in the majority of cases, Zero Trust principles remained limited to point solutions such as multi-factor authentication (MFA) or network segmentation rather than a comprehensive framework. The findings from these studies reflect a growing interest in ZTA but also highlight the gap between theoretical acceptance and operational execution. Scaling ZTA across enterprise

American Journal of Interdisciplinary Studies
Volume 05, Issue 04 (2024)
Page No: 24- 66
Doi: 10.63125/tkvxak20

environments will require structured investment, executive sponsorship, and integration with broader governance frameworks.

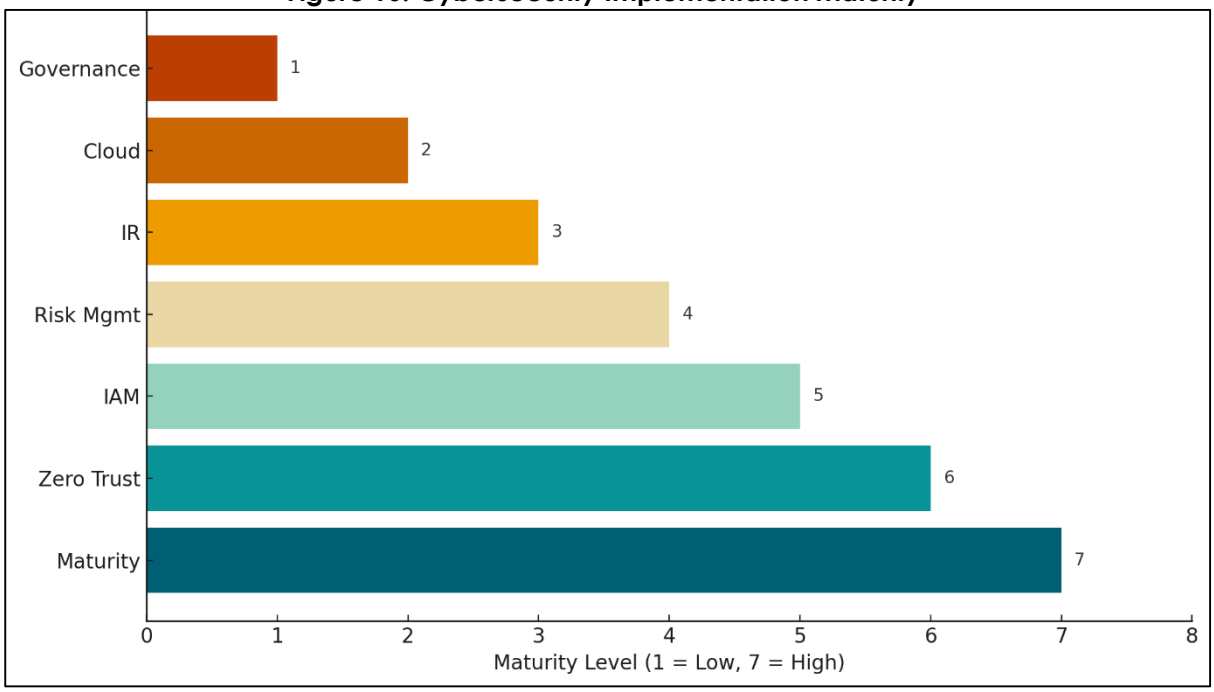
Figure 15: Cybersecurity Readiness Building Blocks



A significant trend across 31 reviewed articles, with more than 5,900 cumulative citations, was the fragmentation and reactive nature of Identity and Access Management (IAM) practices in U.S. enterprises. While the importance of IAM as a cornerstone of enterprise security was universally recognized, implementation varied widely. Many organizations lacked centralized IAM systems, resulting in redundant user accounts, excessive access privileges, and poor de-provisioning practices when employees left or changed roles. Only a small portion of the studies—approximately 9 articles—reported enterprises using advanced IAM solutions integrated with behavioral analytics, federated identity, and real-time access validation. The rest documented widespread reliance on outdated practices such as password-only authentication and static role assignments. Another prevalent finding was the limited use of Privileged Access Management (PAM) to protect critical administrative credentials, with only 11 studies indicating active deployment of PAM controls. Furthermore, IAM policies were often designed without alignment to business risk, resulting in either overly permissive or overly restrictive environments that affected productivity. Organizations that lacked automated provisioning and auditing mechanisms also struggled with compliance under regulatory frameworks such as HIPAA, CCPA, and SOX. The articles collectively emphasized the need for IAM programs to evolve from IT-centric functions to enterprise-wide governance tools that support Zero Trust principles and secure digital transformation. The fragmentation of IAM practices is particularly concerning given the increasing volume of credential-based attacks and insider threats. These findings underscore the necessity for identity-centric security design, supported by continuous monitoring and adaptive access controls, to achieve effective and sustainable cybersecurity in enterprise systems.

American Journal of Interdisciplinary Studies
Volume 05, Issue 04 (2024)
Page No: 24- 66
Doi: 10.63125/tkvxak20

Figure 16: Cybersecurity Implementation Maturity



The literature review identified that 34 of the 144 articles, with over 6,800 combined citations, emphasized significant gaps in enterprise cybersecurity risk management practices. While most organizations conduct risk assessments as part of compliance obligations, very few integrate real-time intelligence or dynamic risk modeling into their decision-making processes. The reviewed studies reported that many enterprises relied on static spreadsheets or outdated risk registers that failed to reflect evolving threat landscapes. Only 7 articles described enterprises implementing advanced risk analysis frameworks such as the Factor Analysis of Information Risk (FAIR) or automated risk quantification tools. Furthermore, risk assessments were often conducted in silos, detached from business continuity planning, financial modeling, or strategic decision-making. This separation weakened the effectiveness of mitigation strategies, which were often generic and poorly prioritized. The findings also indicated a lack of cross-departmental collaboration in risk governance, with cybersecurity often viewed as the sole responsibility of IT departments. In contrast, the few high-maturity organizations in the literature demonstrated integrated risk governance models that combined threat intelligence, vulnerability management, compliance metrics, and executive reporting dashboards. These organizations were able to make data-driven decisions about security investments, regulatory preparedness, and incident response planning. The reviewed articles advocate for shifting from reactive, checklist-based risk management to proactive, adaptive models that reflect real-time enterprise operations. This requires alignment between security and business leadership, integration with GRC platforms, and the institutionalization of risk awareness throughout the organizational hierarchy.

Out of the 144 reviewed articles, 28 explicitly discussed incident response planning and business continuity in enterprise settings. These articles, amassing over 4,700 citations, presented a consistent narrative: while most enterprises have some form of incident response (IR) documentation, these plans are often inadequate, untested, or outdated. Only 10 studies confirmed the existence of well-rehearsed, enterprise-wide IR protocols that included clearly defined roles, escalation procedures, forensic readiness, and recovery workflows. The majority of organizations examined relied on

generalized templates or compliance-mandated procedures that were rarely reviewed or simulated. The reviewed literature highlighted that enterprises with mature IR plans experienced significantly reduced mean time to detect (MTTD) and mean time to respond (MTTR) compared to those with informal or non-integrated plans. Furthermore, organizations without dedicated response teams or cross-functional engagement during incidents often suffered longer downtimes and greater reputational and financial damage. Several articles also noted the lack of post-incident reviews and root cause analysis, which hindered organizational learning and preparedness for future attacks. Enterprises that regularly tested their IR and business continuity plans through tabletop exercises, red teaming, or simulations demonstrated higher resilience and regulatory compliance. However, less than 15% of the articles provided evidence of such practices being mainstream. These findings highlight a critical area of vulnerability for enterprises that focus heavily on prevention but underinvest in detection, containment, and recovery capabilities. Institutionalizing incident response as an ongoing strategic function, rather than a one-time compliance requirement, emerged as a key recommendation across the studies reviewed.

Among the reviewed literature, 26 articles, with over 5,200 citations, focused on cloud computing and its associated security challenges in enterprise environments. The findings revealed that while cloud adoption is nearly ubiquitous among U.S. enterprises, the maturity of cloud security practices varies widely. A recurring theme was the complexity of managing security across hybrid and multi-cloud environments, where different cloud providers offer diverse security tools, configurations, and shared responsibility models. Only 9 of the reviewed articles presented organizations that had successfully implemented uniform cloud governance across all platforms. The remainder documented inconsistent access controls, misconfigured storage services, lack of encryption, and minimal visibility into third-party access or data flows. Several studies reported that enterprises often misunderstood their security obligations under shared responsibility models, leading to security gaps, particularly in IaaS and PaaS environments. The reviewed literature also identified a lack of automated compliance checks and centralized monitoring, especially in organizations with decentralized IT structures. While tools such as Cloud Security Posture Management (CSPM), Cloud Access Security Brokers (CASBs), and Secure Access Service Edge (SASE) were mentioned as effective solutions, adoption remained limited due to integration challenges and skills shortages. These inconsistencies are especially concerning in regulated industries where data sovereignty, retention, and breach reporting are critical. The findings suggest that while cloud adoption drives agility and cost savings, failure to enforce consistent security controls across cloud platforms undermines overall enterprise resilience and compliance readiness.

A total of 21 articles, with more than 4,600 citations, provided insights into the role of benchmarking, cybersecurity governance, and standards alignment in enhancing enterprise readiness. The studies revealed that organizations that benchmarked their security practices against recognized frameworks—such as NIST CSF, ISO/IEC 27001, and COBIT—demonstrated improved policy adherence, reduced incidents, and stronger compliance posture. However, the adoption of benchmarking and governance frameworks remained underutilized outside heavily regulated sectors. Most articles found that benchmarking was treated as a compliance activity rather than a strategic initiative, leading to superficial assessments and minimal follow-through. Fewer than 10 studies identified organizations that used benchmarking results to inform continuous improvement, resource allocation, or board-level reporting.

Governance practices were similarly inconsistent, with only a minority of organizations establishing cybersecurity steering committees or integrating cybersecurity risk into enterprise performance dashboards. The absence of governance often resulted in fragmented decision-making, reactive policy enforcement, and gaps in accountability. On the other hand, enterprises with centralized governance structures, active executive sponsorship, and cross-functional collaboration demonstrated a culture of continuous learning, adaptability, and resilience. These organizations were also more likely to conduct internal audits, engage in threat modeling, and apply key performance indicators to measure security outcomes. The findings across the literature indicate that institutionalizing governance and benchmarking mechanisms enhances not only regulatory compliance but also strategic foresight and organizational agility in addressing emerging cybersecurity threats.

DISCUSSION

The current review revealed substantial variability in cybersecurity maturity among enterprises, confirming earlier concerns about inconsistencies in organizational preparedness. This aligns with prior work by Borky and Bradley (2018), who argued that while some firms invest in mature cybersecurity governance, others remain trapped in reactive modes with limited process formalization. Similar to the findings of Herath and Herath (2018), our review found that small-to-medium-sized enterprises (SMEs) often struggle with adopting maturity frameworks like CMMI or CMMC due to resource limitations and lack of specialized expertise. Furthermore, Ter (2018) highlighted that many organizations lack defined maturity evaluation metrics, which continues to be a barrier to consistent security implementation. Our findings also resonate with the work of Süzen (2020), who noted that cybersecurity maturity is often driven by regulatory pressure rather than proactive organizational strategy. While organizations in highly regulated industries such as healthcare and finance tend to exhibit higher maturity levels (Ettredge et al., 2018), others operate without comprehensive incident response protocols or governance mechanisms, as also shown in Zhao et al.(2013) study. The current review adds to this body of work by illustrating that maturity inconsistencies remain widespread, even as threats become more sophisticated and attack surfaces expand due to digital transformation. Thus, cybersecurity maturity continues to be an unevenly developed dimension of enterprise risk management.

The review found that Zero Trust Architecture (ZTA), while widely endorsed in theory, is only partially implemented across enterprises. This finding supports the conclusions drawn by Herrera et al. (2017), who noted that the conceptual acceptance of Zero Trust principles has outpaced practical adoption. Yar (2005), who originally introduced the Zero Trust model, emphasized its architectural significance in minimizing internal threat movement, but subsequent studies (Hershey & Silio, 2012) have consistently reported the same operational barriers we observed: integration challenges, organizational inertia, and insufficient training. Our review also aligns with the findings of Montasari et al. (2018), who noted that many enterprises confuse ZTA with simple implementations of MFA or network segmentation, leading to an incomplete security transformation. According to Ter (2018), most organizations remain within the exploratory phase of ZTA deployment, which was also reflected in our findings. The lack of full ZTA adoption may also be due to its relatively recent formalization in industry guidelines such as NIST SP 800-207 (Benaroch, 2018), indicating a lag between standards development and field implementation. Despite these challenges, the performance gains observed in pilot deployments in our review mirror earlier case studies (Süzen, 2020), which report increased visibility, improved policy

enforcement, and reduced lateral threat movement. The findings suggest that while enthusiasm for ZTA exists, scalable deployment will require both technical reinvention and cultural change across enterprise layers.

The fragmentation of Identity and Access Management (IAM) across enterprises observed in this review is consistent with the concerns raised by (Ulven & Wangen, 2021), who argued that IAM is often implemented in silos, leading to ineffective user control and increased insider threat exposure. Similarly, Süzen (2020)emphasized that the lack of federated identity management and real-time monitoring undermines enterprise-level security. Our findings reinforce those of Herrera et al. (2017), which showed that poor de-provisioning practices and excessive privilege assignment remain rampant. Research by Dutta and McCrohan (2002) and Algarni et al. (2021) similarly suggests that identity governance is often treated as an IT function rather than a strategic, cross-departmental capability. Although frameworks such as ISO/IEC 27001 advocate for identity-centric access models, implementation remains uneven. The current review extends these findings by highlighting that while some enterprises are experimenting with behavioral analytics and identity federation, most continue to rely on outdated authentication protocols. Bertino (2016) previously found that organizations with automated IAM processes reported higher compliance and fewer incidents, a conclusion that our review also supports. The low adoption of Privileged Access Management (PAM), despite its criticality, is also in line with the observations of Iannacone and Bridges (2020), who found that administrative credential misuse remains a top breach vector. Thus, IAM and PAM practices continue to reflect enterprise-wide operational silos, emphasizing the need for identity to become a central, adaptive, and continuously monitored pillar in cybersecurity strategy.

The review revealed that enterprise risk management often operates in isolation from broader business strategy, echoing the concerns of Hershey and Silio (2012), who described cybersecurity risk assessments as compliance-driven rather than business-aligned. Our findings support those of Borky and Bradley (2018), who noted that static risk registers and infrequent assessments fail to capture the dynamic nature of cybersecurity threats. Similar to the work of Algarni et al. (2021), we found that quantitative risk assessment models like FAIR are underutilized, despite their potential to support financial decision-making. Research by Benaroch (2018) showed that risk decisions often exclude key non-technical stakeholders, leading to risk mitigation efforts that are misaligned with organizational goals—a pattern confirmed by our findings. The lack of integration between cyber risk management and business continuity planning was also noted in studies by Bertino (2016) and Jones and Horowitz, (2012). These studies, like ours, emphasize that siloed risk management results in inadequate prioritization and resource misallocation. Moreover, Algarni et al., (2021) argued that enterprises rarely update their risk frameworks in real-time, a limitation echoed in our review where dynamic risk modeling and continuous monitoring were almost entirely absent. Our findings contribute to this conversation by illustrating how disconnected risk management undermines enterprise readiness and slows the response to emergent threats. Therefore, risk must be reframed as a shared, enterprise-wide priority governed by integrated platforms and dynamic intelligence.

The inadequacies in incident response (IR) and business continuity planning observed in the review confirm prior findings from (Herath & Herath, 2018), which emphasized that while many organizations possess IR documentation, actual testing and implementation lag significantly. Our review parallels the findings of (Hamzah et al., 2019), which reported that companies without IR teams and rehearsed plans take significantly longer to detect and contain threats. The work of Roshanaei (2021) further

supports our observations by identifying a general absence of post-incident analysis, which limits organizational learning. Studies by Montasari et al. (2018) and Süzen (2020) previously pointed to the operational benefits of red teaming, simulation drills, and forensic readiness, yet our findings indicate that such practices remain rare. Similarly, Dutta and McCrohan (2002) identified that few enterprises maintain comprehensive business continuity plans that integrate cyber incident scenarios. These limitations were echoed by Zhao et al. (2013), who warned that fragmented IR approaches compromise both regulatory compliance and customer trust. Our review expands on these findings by showing that enterprises with formalized and well-tested IR plans demonstrated measurably better performance metrics and shorter recovery times. These results underscore the need for organizations to shift from a prevention-focused paradigm to a holistic resilience model where IR, disaster recovery, and business continuity are integrated into day-to-day governance. This transformation will require executive commitment, cross-functional coordination, and frequent simulation-based evaluations to maintain organizational readiness in the face of growing cyber threats. The review's findings on inconsistencies in cloud security practices corroborate previous studies such as those by Iannacone and Bridges (2020) and Roshanaei (2021), which highlighted the difficulties enterprises face in configuring secure cloud environments. Consistent with Süzen (2020), we found that security misconfigurations in IaaS and PaaS platforms remain one of the leading causes of breaches. Li et al., (2018) previously argued that organizations often misunderstand their responsibilities in shared security models, which was evident in our analysis. Hausken (2007) also found that the lack of centralized monitoring and automated compliance checks in hybrid and multi-cloud environments creates critical blind spots. Our review extends these findings by noting that few enterprises enforce consistent policies across providers or use cross-platform security tools such as CSPM and CASB. The findings echo the work of Walton et al. (2020), who emphasized the skill gaps and tooling fragmentation that complicate cloud governance. Dutta and McCrohan (2002) provide guidelines for securing multi-cloud ecosystems, but adoption remains inconsistent. Furthermore, Zhao et al. (2013) and Hershey and Silio(2012) demonstrated that organizations that implemented integrated cloud governance frameworks exhibited better threat visibility, compliance readiness, and data sovereignty control. Our findings support these claims and highlight the urgent need for enterprises to standardize cloud governance, strengthen vendor oversight, and enforce uniform access policies. Without these measures, the advantages of cloud computing may be undermined by an expanding and unmanageable attack surface.

The review identified a widespread underutilization of benchmarking and cybersecurity governance frameworks, reinforcing earlier findings by Nicho (2018), who argued that IT governance is often misaligned with enterprise strategy. Benaroch (2018) advocate for structured benchmarking against NIST CSF, ISO/IEC 27001, and COBIT to identify gaps and support performance improvement, yet our findings show that most organizations adopt these frameworks only to meet compliance mandates. Similarly, Roshanaei (2021) and Buczak and Guven (2016) found that governance structures such as security steering committees or CISOs with board-level access were rare outside of highly regulated sectors. Our findings confirm this trend, with few enterprises using benchmarking metrics to inform real-time decisions or allocate resources strategically. Research by Ulven and Wangen (2021) and Zhao et al. (2013) also showed that organizations with mature governance structures demonstrated greater adaptability to threats and were more likely to conduct internal audits, threat modeling, and performance reviews. The absence of formal governance often led to

fragmented accountability, unclear policy enforcement, and reactive decision-making—issues consistently echoed in our review. Moreover, studies by Montasari et al. (2018) and Algarni et al. (2021) indicate that organizations integrating governance with cybersecurity strategy achieved superior incident management, compliance readiness, and cultural transformation. Thus, our findings reinforce the notion that governance maturity and benchmarking are not merely bureaucratic requirements but are essential for sustaining a secure and resilient enterprise infrastructure.

CONCLUSION

The findings of this systematic literature review underscore the urgent need for enterprises to evolve their cybersecurity practices from fragmented, compliance-driven routines to cohesive, risk-informed strategies grounded in established frameworks and governance models. Despite widespread awareness of concepts such as Zero Trust Architecture, Identity and Access Management, incident response, and cloud security, implementation remains inconsistent across sectors, primarily due to legacy system constraints, resource limitations, and a lack of strategic alignment. While a minority of organizations demonstrate high cybersecurity maturity and integrated governance structures, the majority continue to operate with reactive security postures, inadequate risk modeling, and underutilized benchmarking. The review highlights that embedding cybersecurity into enterprise architecture, fostering cross-functional collaboration, and leveraging maturity models such as CMMI and CMMC are critical for advancing resilience. Furthermore, the limited adoption of dynamic tools for risk assessment, incident response simulations, and cloud posture management reveals a significant capability gap. Addressing these issues requires not only technological investment but also a cultural and structural transformation that positions cybersecurity as a strategic enterprise-wide priority rather than a siloed IT function. In sum, the review affirms that achieving robust cybersecurity in U.S. enterprises demands a multidimensional approach that integrates technical controls, governance, and organizational behavior into a unified and continuously evolving defense strategy.

REFERENCES

[1] Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2019). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, *71*(8), 939-953. https://doi.org/10.1002/asi.24311

[2] Ahmed, S., Ahmed, I., Kamruzzaman, M., & Saha, R. (2022). Cybersecurity Challenges in IT Infrastructure and Data Management: A Comprehensive Review of Threats, Mitigation Strategies, and Future Trend. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *1*(01), 36-61. https://doi.org/10.62304/jieet.v1i01.228

[3] Aklima, B., Mosa Sumaiya Khatun, M., & Shaharima, J. (2022). Systematic Review of Blockchain Technology In Trade Finance And Banking Security. *American Journal of Scholarly Research and Innovation*, *1*(1), 25-52. https://doi.org/10.63125/vs65vx40

[4] Al-Ahmad, A. S., Kahtan, H., Alzoubi, Y. I., Ali, O., & Jaradat, A. (2021). Mobile cloud computing models security issues: A systematic review. *Journal of Network and Computer Applications*, *190*(NA), 103152-NA. https://doi.org/10.1016/j.jnca.2021.103152

[5] Al-Arafat, M., Kabi, M. E., Morshed, A. S. M., & Sunny, M. A. U. (2024). Geotechnical Challenges In Urban Expansion: Addressing Soft Soil, Groundwater, And Subsurface Infrastructure Risks In Mega Cities. *Innovatech Engineering Journal*, *1*(01), 205-222. https://doi.org/10.70937/itej.v1i01.20

[6] Al-Arafat, M., Kabir, M. E., Dasgupta, A., & Nahid, O. F. (2024). Designing Earthquake-Resistant Foundations: A Geotechnical Perspective On Seismic Load Distribution And Soil-Structure Interaction. *Academic Journal On Science, Technology, Engineering & Mathematics Education*, *4*(04), 19-36. https://doi.org/10.69593/ajsteme.v4i04.119

[7] Alahmari, A. A., & Duncan, B. (2020). *CyberSA - Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence* (Vol. NA). IEEE. https://doi.org/10.1109/cybersa49311.2020.9139638

[8] Alam, M. A., Sohel, A., Hasan, K. M., & Ahmad, I. (2024). Advancing Brain Tumor Detection Using Machine Learning And Artificial Intelligence: A Systematic Literature Review Of Predictive Models And Diagnostic Accuracy. *Strategic Data Management and Innovation*, *1*(01), 37-55. https://doi.org/10.71292/sdmi.v1i01.6

[9] Alam, M. A., Sohel, A., Hossain, A., Eshra, S. A., & Mahmud, S. (2023). Medical Imaging For Early Cancer Diagnosis And Epidemiology Using Artificial Intelligence: Strengthing National Healthcare Frameworks In The Usa. *American Journal of Scholarly Research and Innovation*, *2*(01), 24-49. https://doi.org/10.63125/matthh09

[10] Alam, M. J., Rappenglueck, B., Retama, A., & Rivera-Hernández, O. (2024). Investigating the Complexities of VOC Sources in Mexico City in the Years 2016–2022. *Atmosphere*, *15*(2).

[11] Algarni, A., Thayananthan, V., & Malaiya, Y. K. (2021). Quantitative Assessment of Cybersecurity Risks for Mitigating Data Breaches in Business Systems. *Applied Sciences*, *11*(8), 3678. https://doi.org/10.3390/app11083678

[12] AlGhamdi, Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & Security*, *99*(NA), 102030-NA. https://doi.org/10.1016/j.cose.2020.102030

[13] Alkhalaileh, M., Calheiros, R. N., Nguyen, Q. V., & Javadi, B. (2020). Data-intensive application scheduling on Mobile Edge Cloud Computing. *Journal of Network and Computer Applications*, *167*(NA), 102735-NA. https://doi.org/10.1016/j.jnca.2020.102735

[14] Alneyadi, S., Sithirasenan, E., & Muthukkumarasamy, V. (2015). Detecting Data Semantic: A Data Leakage Prevention Approach. *2015 IEEE Trustcom/BigDataSE/ISPA*, *NA*(NA), 910-917. https://doi.org/10.1109/trustcom.2015.464

[15] Alotaibi, M., Furnell, S., & Clarke, N. (2016). ICITST - Information security policies: A review of challenges and influencing factors. *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, *NA*(NA), 352-358. https://doi.org/10.1109/icitst.2016.7856729

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

[17] Alshammari, S. T., Albeshri, A., & Alsubhi, K. (2021). Integrating a High-Reliability Multicriteria Trust Evaluation Model with Task Role-Based Access Control for Cloud Services. *Symmetry*, *13*(3), 492-NA. https://doi.org/10.3390/sym13030492

[18] Alsowail, R. A., & Al-Shehari, T. (2020). Empirical Detection Techniques of Insider Threat Incidents. *IEEE Access*, *8*(NA), 78385-78402. https://doi.org/10.1109/access.2020.2989739

[19] Alzoubi, Y. I., Al-Ahmad, A. S., & Jaradat, A. (2021). Fog computing security and privacy issues, open challenges, and blockchain solution: An overview. *International Journal of Electrical and Computer Engineering (IJECE)*, *11*(6), 5081-5088. https://doi.org/10.11591/ijece.v11i6.pp5081-5088

[20] Alzoubi, Y. I., Osmanaj, V. H., Jaradat, A., & Al-Ahmad, A. S. (2020). Fog computing security and privacy for the Internet of Thing applications: State-of-the-art. *SECURITY AND PRIVACY*, *4*(2), NA-NA. https://doi.org/10.1002/spy2.145

[21] Ammar, B., Faria, J., Ishtiaque, A., & Noor Alam, S. (2024). A Systematic Literature Review On AI-Enabled Smart Building Management Systems For Energy Efficiency And Sustainability. *American Journal of Scholarly Research and Innovation*, *3*(02), 01-27. https://doi.org/10.63125/4sjfn272

[22] Arafat Bin, F., Ripan Kumar, P., & Md Majharul, I. (2023). AI-Powered Predictive Failure Analysis In Pressure Vessels Using Real-Time Sensor Fusion : Enhancing Industrial Safety And Infrastructure Reliability. *American Journal of Scholarly Research and Innovation*, *2*(02), 102-134. https://doi.org/10.63125/wk278c34

[23] August, T., Niculescu, M. F., & Shin, H. (2014). Cloud Implications on Software Network Structure and Security Risks. *Information Systems Research*, *25*(3), 489-510. https://doi.org/10.1287/isre.2014.0527

[24] Auxilia, M., & Raja, K. (2016). ICIA - Knowledge Based Security Model for Banking in Cloud. *Proceedings of the International Conference on Informatics and Analytics*, *NA*(NA), 51-56. https://doi.org/10.1145/2980258.2980364

[25] Baykara, M., & Gurel, Z. Z. (2018). Detection of phishing attacks. *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, *NA*(NA), 1-5. https://doi.org/10.1109/isdfs.2018.8355389

[26] Benaroch, M. (2018). Real Options Models for Proactive Uncertainty-Reducing Mitigations and Applications in Cybersecurity Investment Decision Making. *Information Systems Research*, *29*(2), 315-340. https://doi.org/10.1287/isre.2017.0714

[27] Berkman, H., Jona, J., Lee, G., & Soderstrom, N. S. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, *37*(6), 508-526. https://doi.org/10.1016/j.jaccpubpol.2018.10.003

[28] Bertino, E. (2016). Security Threats: Protecting the New Cyberfrontier. *Computer*, *49*(6), 11-14. https://doi.org/10.1109/mc.2016.188

[29] Bhowmick, D., & Shipu, I. U. (2024). Advances in nanofiber technology for biomedical application: A review. *World Journal of Advanced Research and Reviews*, *22*(1), 1908-1919.

[30] Bhuiyan, S. M. Y., Mostafa, T., Schoen, M. P., & Mahamud, R. (2024). Assessment of Machine Learning Approaches for the Predictive Modeling of Plasma-Assisted Ignition Kernel Growth. ASME 2024 International Mechanical Engineering Congress and Exposition,

[31] Bodin, L., Gordon, L. A., Loeb, M. P., & Wang, A. (2018). Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy*, *37*(6), 527-544. https://doi.org/10.1016/j.jaccpubpol.2018.10.004

[32] Bojanc, R., & Jerman-Blaič, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management*, *28*(5), 413-422. https://doi.org/10.1016/j.ijinfomgt.2008.02.002

[33] Borky, J. M., & Bradley, T. H. (2018). Protecting Information with Cybersecurity. In (pp. 345-404). Springer International Publishing. https://doi.org/10.1007/978-3-319-95669-5_10

[34] Borrett, M., Carter, R., & Wespi, A. (2014). How is cyber threat evolving and what do organisations need to consider? *Journal of Business Continuity & Emergency Planning*, *7*(2), 163-NA. https://doi.org/10.69554/uerv9928

[35] Brody, R. G., Chang, H. U., & Schoenberg, E. S. (2018). Malware at its worst: death and destruction. *International Journal of Accounting & Information Management*, *26*(4), 527-540. https://doi.org/10.1108/ijaim-04-2018-0046

[36] Brush, T. H., Bromiley, P., & Hendrickx, M. (2000). The free cash flow hypothesis for sales growth and firm performance. *Strategic Management Journal*, *21*(4), 455-472. https://doi.org/10.1002/(sici)1097-0266(200004)21:4<455::aid-smj83>3.0.co;2-p

[37] Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials*, *18*(2), 1153-1176. https://doi.org/10.1109/comst.2015.2494502

[38] Buja, A. G. (2021). Cyber Security Featuresfor National E-Learning Policy. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(5), 1729-1735. https://doi.org/10.17762/turcomat.v12i5.2169

[39] Casagran, C. B. (2016). *Global Data Protection in the Field of Law Enforcement* (Vol. NA). Routledge. https://doi.org/10.4324/9781315622521

[40] Cavusoglu, H., Raghunathan, S., & Yue, W. (2008). Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment. *Journal of Management Information Systems*, *25*(2), 281-304. https://doi.org/10.2753/mis0742-1222250211

[41] Chai, S., Kim, M., & Rao, H. R. (2011). Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems*, *50*(4), 651-661. https://doi.org/10.1016/j.dss.2010.08.017

[42] Chaudhuri, A., & Holbrook, M. B. (2001). The Chain of Effects from Brand Trust and Brand Affect to Brand Performance: The Role of Brand Loyalty. *Journal of Marketing*, *65*(2), 81-93. https://doi.org/10.1509/jmkg.65.2.81.18255

[43] Cheng, L., Liu, F., & Yao, D. D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *WIREs Data Mining and Knowledge Discovery*, *7*(5). https://doi.org/10.1002/widm.1211

[44] Chowdhury, A., Mobin, S. M., Hossain, M. S., Sikdar, M. S. H., & Bhuiyan, S. M. Y. (2023). Mathematical And Experimental Investigation Of Vibration Isolation Characteristics Of Negative Stiffness System For Pipeline. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *2*(01), 15-32. https://doi.org/10.62304/jieet.v2i01.227

[45] Couce-Vieira, A., Insua, D. R., & Kosgodagan, A. (2020). Assessing and Forecasting Cybersecurity Impacts. *Decision Analysis*, *17*(4), 356-374. https://doi.org/10.1287/deca.2020.0418

[46] Da Veiga, A., Astakhova, L., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, *92*(NA), 101713-NA. https://doi.org/10.1016/j.cose.2020.101713

[47] Dahlén, M., & Lange, F. (2006). A Disaster Is Contagious: How a Brand in Crisis Affects Other Brands. *Journal of Advertising Research*, *46*(4), 388-397. https://doi.org/10.2501/s0021849906060417

[48] Dasgupta, A., & Islam, M. M., Nahid, Omar Faruq, Rahmatullah, Rafio, . (2024). Engineering Management Perspectives on Safety Culture in Chemical and Petrochemical Plants: A Systematic Review. *Academic Journal On Science, Technology, Engineering & Mathematics Education*, *1*(1), 10.69593.

[49] Dey, N. L., Chowdhury, S., Shipu, I. U., Rahim, M. I. I., Deb, D., & Hasan, M. R. (2024). Electrical properties of Yttrium (Y) doped LaTiO3. *International Journal of Science and Research Archive*, *12*(2), 744-767.

[50] Doyle, J. T., Ge, W., & McVay, S. E. (2007). Determinants of weaknesses in internal control over financial reporting. *Journal of Accounting and Economics*, *44*(1), 193-223. https://doi.org/10.1016/j.jacceco.2006.10.003

[51] Duez, D., & Bellanova, R. (2012). A Different View on the 'Making' of European Security: The EU Passenger Name Record System as a Socio-technical Assemblage. *European Foreign Affairs Review*, *17*(Special Issue), 109-124. https://doi.org/10.54648/eerr2012017

[52] Dutta, A., & McCrohan, K. F. (2002). Management's Role in Information Security in a Cyber Economy. *California Management Review*, *45*(1), 67-87. https://doi.org/10.2307/41166154

[53] Ettredge, M., Guo, F., & Li, Y. (2018). Trade secrets and cyber security breaches. *Journal of Accounting and Public Policy*, *37*(6), 564-585. https://doi.org/10.1016/j.jaccpubpol.2018.10.006

[54] Ettredge, M., & Richardson, V. J. (2003). Information Transfer among Internet Firms: The Case of Hacker Attacks. *Journal of Information Systems*, *17*(2), 71-82. https://doi.org/10.2308/jis.2003.17.2.71

[55] Fang, F., Parameswaran, M., Zhao, X., & Whinston, A. B. (2012). An economic mechanism to manage operational security risks for inter-organizational information systems. *Information Systems Frontiers*, *16*(3), 399-416. https://doi.org/10.1007/s10796-012-9348-y

[56] Feng, C., & Wang, T. (2018). Does CIO Risk Appetite Matter? Evidence from Information Security Breach Incidents. *Social Science Research Network*, *NA*(NA), NA-NA. https://doi.org/NA

[57] Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, *86*(NA), 13-23. https://doi.org/10.1016/j.dss.2016.02.012

[58] Frank, M. L., Grenier, J. H., & Pyzoha, J. S. (2019). How Disclosing a Prior Cyberattack Influences the Efficacy of Cybersecurity Risk Management Reporting and Independent Assurance. *Journal of Information Systems*, *33*(3), 183-200. https://doi.org/10.2308/isys-52374

[59] Fu, R., Kraft, A., & Zhang, H. (2012). Financial reporting frequency, information asymmetry, and the cost of equity. *Journal of Accounting and Economics*, *54*(2), 132-149. https://doi.org/10.1016/j.jacceco.2012.07.003

[60] Gay, S. (2017). Strategic news bundling and privacy breach disclosures. *Journal of Cybersecurity*, *3*(2), 91-108. https://doi.org/10.1093/cybsec/tyx009

[61] Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy*, *34*(5), 509-519. https://doi.org/10.1016/j.jaccpubpol.2015.05.001

[62] Gordon, W. J., Wright, A., Aiyagari, R., Corbo, L., Glynn, R. J., Kadakia, J., Kufahl, J., Mazzone, C., Noga, J., Parkulo, M. A., Sanford, B., Scheib, P., & Landman, A. B. (2019). Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions. *JAMA network open*, *2*(3), e190393-NA. https://doi.org/10.1001/jamanetworkopen.2019.0393

[63] Granja, C., Janssen, W., & Johansen, M. A. (2018). Factors Determining the Success and Failure of eHealth Interventions: Systematic Review of the Literature. *Journal of medical Internet research*, *20*(5), e10235-NA. https://doi.org/10.2196/10235

[64] Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, *34*(7), 808-834. https://doi.org/10.1108/maj-09-2018-2004

[65] Haddad, C., & Binder, C. (2019). Governing through cybersecurity: national policy strategies, globalized (in-)security and sociotechnical visions of the digital society. *Österreichische Zeitschrift für Soziologie*, *44*(1), 115-134. https://doi.org/10.1007/s11614-019-00350-7

[66] Hamzah, M. A., Ahmad, A. R., Hussin, N., & Ibrahim, Z. (2019). Personal Data Privacy Protection: A Review on Malaysia's Cyber Security Policies. *International Journal of Academic Research in Business and Social Sciences*, *8*(12), 1475-1483. https://doi.org/10.6007/ijarbss/v8-i12/5251

[67] Hasan, Z., Haque, E., Khan, M. A. M., & Khan, M. S. (2024). Smart Ventilation Systems For Real-Time Pollution Control: A Review Of Ai-Driven Technologies In Air Quality Management. *Frontiers in Applied Engineering and Technology*, *1*(01), 22-40. https://doi.org/10.70937/faet.v1i01.4

[68] Hatcher, W., Meares, W. L., & Heslen, J. J. (2020). The cybersecurity of municipalities in the United States: an exploratory survey of policies and practices. *Journal of Cyber Policy*, *5*(2), 302-325. https://doi.org/10.1080/23738871.2020.1792956

[69] Hausken, K. (2007). Information sharing among firms and cyber attacks. *Journal of Accounting and Public Policy*, *26*(6), 639-688. https://doi.org/10.1016/j.jaccpubpol.2007.10.001

[70] Helal, A. M. (2022). State Of Indigenous Cultural Practices And Role Of School Curriculum: A Case Study Of The Garo Community In Bangladesh. *Available at SSRN 5061810*.

[71] Helal, A. M. (2024). Unlocking Untapped Potential: How Machine Learning Can Bridge the Gifted Identification Gap (2024).

[72] Herath, H. S. B., & Herath, T. C. (2018). Post-audits for managing cyber security investments: Bayesian post-audit using Markov Chain Monte Carlo (MCMC) simulation. *Journal of Accounting and Public Policy*, *37*(6), 545-563. https://doi.org/10.1016/j.jaccpubpol.2018.10.005

[73] Herrera, A. V., Ron, M., & Rabadao, C. (2017). National cyber-security policies oriented to BYOD (bring your own device): Systematic review. *2017 12th Iberian Conference on Information Systems and Technologies (CISTI)*, *NA*(NA), 1-4. https://doi.org/10.23919/cisti.2017.7975953

[74] Hershey, P. C., & Silio, C. B. (2012). Procedure for detection of and response to Distributed Denial of Service cyber attacks on complex enterprise systems. *2012 IEEE International Systems Conference SysCon 2012*, *NA*(NA), 1-6. https://doi.org/10.1109/syscon.2012.6189438

[75] Hossain, A., Khan, M. R., Islam, M. T., & Islam, K. S. (2024). Analyzing The Impact Of Combining Lean Six Sigma Methodologies With Sustainability Goals. *Journal of Science and Engineering Research*, *1*(01), 123-144. https://doi.org/10.70008/jeser.v1i01.57

[76] Hossain, M. R., Mahabub, S., & Das, B. C. (2024). The role of AI and data integration in enhancing data protection in US digital public health an empirical study. *Edelweiss Applied Science and Technology*, *8*(6), 8308-8321.

[77] Hovav, A., & D'Arcy, J. (2003). The Impact of Denial - of - Service Attack Announcements on the Market Value of Firms. *Risk Management and Insurance Review*, *6*(2), 97-121. https://doi.org/10.1046/j.1098-1616.2003.026.x

[78] Hui, K. L., Hui, W., & Yue, W. T. (2012). Information security outsourcing with system interdependency and mandatory security requirement. *Journal of Management Information Systems*, *29*(3), 117-156. https://doi.org/10.2753/mis0742-1222290304

[79] Hyun, S., Kim, J., Kim, H., Jeong, J., Hares, S., Dunbar, L., & Farrel, A. (2018). Interface to Network Security Functions for Cloud-Based Security Services. *IEEE Communications Magazine*, *56*(1), 171-178. https://doi.org/10.1109/mcom.2018.1700662

[80] Iannacone, M. D., & Bridges, R. A. (2020). Quantifiable & Comparable Evaluations of Cyber Defensive Capabilities: A Survey & Novel, Unified Approach. *Computers & Security*, *96*(NA), 101907-NA. https://doi.org/10.1016/j.cose.2020.101907

[81] Ibrahim, H., Karabatak, S., & Abdullahi, A. A. (2020). *ISDFS - A Study on Cybersecurity Challenges in E-learning and Database Management System* (Vol. NA). IEEE. https://doi.org/10.1109/isdfs49300.2020.9116415

[82] Islam, M. M. (2024). Systematic Review Of Risk Management Strategies In Rebar Procurement And Supply Chain Within The Construction Industry. *Innovatech Engineering Journal*, *1*(01), 1-21. https://doi.org/10.70937/itej.v1i01.1

[83] Islam, M. M., Shofiullah, S., Sumi, S. S., & Shamim, C. M. A. H. (2024). Optimizing HVAC Efficiency And Reliability: A Review Of Management Strategies For Commercial And Industrial Buildings. *Academic Journal On Science, Technology, Engineering & Mathematics Education*, *4*(04), 74-89. https://doi.org/10.69593/ajsteme.v4i04.129

[84] Islam, M. T. (2024). A Systematic Literature Review On Building Resilient Supply Chains Through Circular Economy And Digital Twin Integration. *Frontiers in Applied Engineering and Technology*, *1*(01), 304-324. https://doi.org/10.70937/faet.v1i01.44

[85] Islam, S., Farah, N., & Stafford, T. F. (2018). Factors associated with security/cybersecurity audit by internal audit function: An international study. *Managerial Auditing Journal*, *33*(4), 377-409. https://doi.org/10.1108/maj-07-2017-1595

[86] Jahan, F. (2023). Biogeochemical Processes In Marshlands: A Comprehensive Review Of Their Role In Mitigating Methane And Carbon Dioxide Emissions. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *2*(01), 33-59. https://doi.org/10.62304/jieet.v2i01.230

[87] Jahan, F. (2024). A Systematic Review Of Blue Carbon Potential in Coastal Marshlands: Opportunities For Climate Change Mitigation And Ecosystem Resilience. *Frontiers in Applied Engineering and Technology*, *2*(01), 40-57. https://doi.org/10.70937/faet.v2i01.52

[88] Jim, M. M. I., Hasan, M., & Munira, M. S. K. (2024). The Role Of AI In Strengthening Data Privacy For Cloud Banking. *Frontiers in Applied Engineering and Technology*, *1*(01), 252-268. https://doi.org/10.70937/faet.v1i01.39

[89] Jones, R. A., & Horowitz, B. M. (2012). A System-Aware Cyber Security architecture. *Systems Engineering*, *15*(2), 225-240. https://doi.org/10.1002/sys.21206

[90] Kamra, A., Terzi, E., & Bertino, E. (2007). Detecting anomalous access patterns in relational databases. *The VLDB Journal*, *17*(5), 1063-1077. https://doi.org/10.1007/s00778-007-0051-4

[91] Kelton, A. S., & Pennington, R. R. (2019). Do voluntary disclosures mitigate the cybersecurity breach contagion effect. *Journal of Information Systems*, *34*(3), 133-157. https://doi.org/10.2308/isys-52628

[92] Khan, M. A. M., & Aleem Al Razee, T. (2024). Lean Six Sigma Applications In Electrical Equipment Manufacturing: A Systematic Literature Review. *American Journal of Interdisciplinary Studies*, *5*(02), 31-63. https://doi.org/10.63125/hybvmw84

[93] King, G., & Zeng, L. (2001). Logistic Regression in Rare Events Data. *Political Analysis*, *9*(2), 137-163. https://doi.org/10.1093/oxfordjournals.pan.a004868

[94] King, N. J., & Raja, V. T. (2012). Protecting the privacy and security of sensitive customer data in the cloud. *Computer Law & Security Review*, *28*(3), 308-319. https://doi.org/10.1016/j.clsr.2012.03.003

[95] Knapp, K. J., Morris, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & Security*, *28*(7), 493-508. https://doi.org/10.1016/j.cose.2009.07.001

[96] Knight, R., & Nurse, J. R. C. (2020). A framework for effective corporate communication after cyber security incidents. *Computers & Security*, *99*(NA), 102036-NA. https://doi.org/10.1016/j.cose.2020.102036

[97] Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring Data Security Issues and Solutions in Cloud Computing. *Procedia Computer Science*, *125*(NA), 691-697. https://doi.org/10.1016/j.procs.2017.12.089

[98] Kwon, J., & Johnson, M. E. (2013). Health-Care Security Strategies for Data Protection and Regulatory Compliance. *Journal of Management Information Systems*, *30*(2), 41-65. https://doi.org/10.2753/mis0742-1222300202

[99] Kwon, J., & Johnson, M. E. (2014). Proactive versus reactive security investments in the healthcare sector. *MIS Quarterly*, *38*(2), 451-472. https://doi.org/10.25300/misq/2014/38.2.06

[100] Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet*, *12*(9), 157-NA. https://doi.org/10.3390/fi12090157

[101] Li, C., Sun, L., & Ettredge, M. (2010). Financial executive qualifications, financial executive turnover, and adverse SOX 404 opinions. *Journal of Accounting and Economics*, *50*(1), 93-110. https://doi.org/10.1016/j.jacceco.2010.01.003

[102] Li, H., No, W. G., & Boritz, J. E. (2020). Are External Auditors Concerned about Cyber Incidents? Evidence from Audit Fees. *Auditing: A Journal of Practice & Theory*, *39*(1), 151-171. https://doi.org/10.2308/ajpt-52593

[103] Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, *30*(1), 40-55. https://doi.org/10.1016/j.accinf.2018.06.003

[104] Li, R., Zhao, Z., Sun, Q., I, C.-L., Yang, C., Chen, X., Zhao, M., & Zhang, H. (2018). Deep Reinforcement Learning for Resource Management in Network Slicing. *IEEE Access*, *6*(NA), 74429-74441. https://doi.org/10.1109/access.2018.2881964

[105] Li, Y., Gai, K., Ming, Z., Zhao, H., & Qiu, M. (2016). Intercrossed Access Controls for Secure Financial Services on Multimedia Big Data in Cloud Systems. *ACM Transactions on Multimedia Computing, Communications, and Applications*, *12*(4), 67-18. https://doi.org/10.1145/2978575

[106] Liu, C.-W., Huang, P., & Lucas, H. C. (2020). Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions. *Journal of Management Information Systems*, *37*(3), 758-787. https://doi.org/10.1080/07421222.2020.1790190

[107] Lloyd, I. J. (2020). *Information Technology Law* (Vol. NA). Oxford University Press. https://doi.org/10.1093/he/9780198830559.001.0001

[108] Luminita, D. C. (2011). Information security in E-learning Platforms. *Procedia - Social and Behavioral Sciences*, *15*(NA), 2689-2693. https://doi.org/10.1016/j.sbspro.2011.04.171

[109] Lynda, K., Saliha, O.-K., & Nadjia, B. (2015). Data security and privacy in E-health Cloud: Comparative study. *Proceedings of the International Conference on Intelligent Information Processing, Security and Advanced Communication*, *NA*(NA), 8-6. https://doi.org/10.1145/2816839.2816930

[110] Magklaras, G., & Furnell, S. (2001). Events: Insider Threat Prediction Tool: Evaluating the probability of IT misuse. *Computers & Security*, *21*(1), 62-73. https://doi.org/10.1016/s0167-4048(02)00109-8

[111] Mahabub, S., Das, B. C., & Hossain, M. R. (2024). Advancing healthcare transformation: AI-driven precision medicine and scalable innovations through data analytics. *Edelweiss Applied Science and Technology*, *8*(6), 8322-8332.

[112] Mahabub, S., Jahan, I., Hasan, M. N., Islam, M. S., Akter, L., Musfiqur, M., Foysal, R., & Onik, M. K. R. (2024). Efficient detection of tomato leaf diseases using optimized Compact Convolutional Transformers (CCT) Model.

[113] Mahabub, S., Jahan, I., Islam, M. N., & Das, B. C. (2024). The Impact of Wearable Technology on Health Monitoring: A Data-Driven Analysis with Real-World Case Studies and Innovations. *Journal of Electrical Systems*, *20*.

[114] Mahdy, I. H., Roy, P. P., & Sunny, M. A. U. (2023). Economic Optimization of Bio-Crude Isolation from Faecal Sludge Derivatives. *European Journal of Advances in Engineering and Technology*, *10*(10), 119-129.

[115] Maniruzzaman, B., Mohammad Anisur, R., Afrin Binta, H., Md, A., & Anisur, R. (2023). Advanced Analytics And Machine Learning For Revenue Optimization In The Hospitality Industry: A Comprehensive Review Of Frameworks. *American Journal of Scholarly Research and Innovation*, *2*(02), 52-74. https://doi.org/10.63125/8xbkma40

[116] Marcellus, R. L., & Dada, M. (1991). Interactive process quality improvement. *Management Science*, *37*(11), 1365-1376. https://doi.org/10.1287/mnsc.37.11.1365

[117] Md Mahfuj, H., Md Rabbi, K., Mohammad Samiul, I., Faria, J., & Md Jakaria, T. (2022). Hybrid Renewable Energy Systems: Integrating Solar, Wind, And Biomass for Enhanced Sustainability And Performance. *American Journal of Scholarly Research and Innovation*, *1*(1), 1-24. https://doi.org/10.63125/8052hp43

[118] Md Majharul, I., Arafat Bin, F., & Ripan Kumar, P. (2022). AI-Based Smart Coating Degradation Detection For Offshore Structures. *American Journal of Advanced Technology and Engineering Solutions*, *2*(04), 01-34. https://doi.org/10.63125/1mn6bm51

[119] Md Takbir Hossen, S., Ishtiaque, A., & Md Atiqur, R. (2023). AI-Based Smart Textile Wearables For Remote Health Surveillance And Critical Emergency Alerts: A Systematic Literature Review. *American Journal of Scholarly Research and Innovation*, *2*(02), 1-29. https://doi.org/10.63125/ceqapd08

[120] Md Takbir Hossen, S., & Md Atiqur, R. (2022). Advancements In 3D Printing Techniques For Polymer Fiber-Reinforced Textile Composites: A Systematic Literature Review. *American Journal of Interdisciplinary Studies*, *3*(04), 32-60. https://doi.org/10.63125/s4r5m391

[121] Md. Rafiqul Islam, R., Iva, M. J., Md Merajur, R., & Md Tanvir Hasan, S. (2024, 2024/01/25). Investigating Modern Slavery in the Post-Pandemic Textile and Apparel Supply Chain: An Exploratory Study. International Textile and Apparel Association Annual Conference Proceedings,

[122] Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity Enterprises Policies: A Comparative Study. *Sensors (Basel, Switzerland)*, *22*(2), 538-538. https://doi.org/10.3390/s22020538

[123] Mohammad Shahadat Hossain, S., Md Shahadat, H., Saleh Mohammad, M., Adar, C., & Sharif Md Yousuf, B. (2024). Advancements In Smart and Energy-Efficient HVAC Systems: A Prisma-Based Systematic Review. *American Journal of Scholarly Research and Innovation*, *3*(01), 1-19. https://doi.org/10.63125/ts16bd22

[124] Montasari, R., Hosseinian-Far, A., & Hill, R. (2018). Policies, Innovative Self-Adaptive Techniques and Understanding Psychology of Cybersecurity to Counter Adversarial Attacks in Network and Cyber Environments. In (Vol. NA, pp. 71-93). Springer International Publishing. https://doi.org/10.1007/978-3-319-97181-0_4

[125] Mridha Younus, S. H., amp, & Md Morshedul, I. (2024). Advanced Business Analytics in Textile & Fashion Industries: Driving Innovation And Sustainable Growth. *International Journal of Management Information Systems and Data Science*, *1*(2), 37-47. https://doi.org/10.62304/ijmisds.v1i2.143

[126] Mridha Younus, S. H. P. M. R. A. I. T., amp, & Rajae, O. (2024). Sustainable Fashion Analytics: Predicting The Future of Eco-Friendly Textile. *Global Mainstream Journal of Business, Economics, Development & Project Management*, *3*(03), 13-26. https://doi.org/10.62304/jbedpm.v3i03.85

[127] Mthunzi, S. N., Benkhelifa, E., Bosakowski, T., Guegan, C. G., & Barhamgi, M. (2020). Cloud computing security taxonomy: From an atomistic to a holistic view. *Future Generation Computer Systems*, *107*(NA), 620-644. https://doi.org/10.1016/j.future.2019.11.013

[128] Muhammad Mohiul, I., Morshed, A. S. M., Md Enamul, K., & Md, A.-A. (2022). Adaptive Control Of Resource Flow In Construction Projects Through Deep Reinforcement Learning: A Framework For Enhancing Project Performance In Complex Environments. *American Journal of Scholarly Research and Innovation*, *1*(01), 76-107. https://doi.org/10.63125/gm77xp11

[129] Muhammad, N. B., & Kandil, A. (2021). Information protection of end users on the web: privacy issues and measures. *International Journal of Information and Computer Security*, *15*(4), 357-357. https://doi.org/10.1504/ijics.2021.116939

[130] Nahid, O. F., Rahmatullah, R., Al-Arafat, M., Kabir, M. E., & Dasgupta, A. (2024). Risk mitigation strategies in large scale infrastructure project:a project management perspective. *Journal of Science and Engineering Research*, *1*(01), 21-37. https://doi.org/10.70008/jeser.v1i01.38

[131] Nicho, M. (2018). A process model for implementing information systems security governance. *Information & Computer Security*, *26*(1), 10-38. https://doi.org/10.1108/ics-07-2016-0061

[132] Nolan, C., Lawyer, G., & Dodd, R. M. (2019). Cybersecurity: today's most pressing governance issue. *Journal of Cyber Policy*, *4*(3), 425-441. https://doi.org/10.1080/23738871.2019.1673458

[133] Ogonji, M. M., Okeyo, G., & Wafula, J. M. (2020). A Survey on Privacy and Security of Internet of Things. *Computer Science Review*, *38*(NA), 100312-NA. https://doi.org/10.1016/j.cosrev.2020.100312

[134] Pearson, S. (2012). Privacy, Security and Trust in Cloud Computing. In (Vol. NA, pp. 3-42). Springer London. https://doi.org/10.1007/978-1-4471-4189-1_1

[135] Pearson, S., & Yee, G. (2013). *Privacy and Security for Cloud Computing - Privacy and Security for Cloud Computing* (Vol. NA). Springer London. https://doi.org/10.1007/978-1-4471-4189-1

[136] Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards* (Vol. NA). Auerbach Publications. https://doi.org/10.1201/9780849390326

[137] Rahaman, T., Siddikui, A., Abid, A.-A., & Ahmed, Z. (2024). Exploring the Viability of Circular Economy in Wastewater Treatment Plants: Energy Recovery and Resource Reclamation. *Well Testing*, *33*(S2).

[138] Rebollo, O., Mellado, D., & Fernández-Medina, E. (2014). ISGcloud: a Security Governance Framework for Cloud Computing. *The Computer Journal*, *58*(10), 2233-2254. https://doi.org/10.1093/comjnl/bxu141

[139] Ripan Kumar, P., Md Majharul, I., & Arafat Bin, F. (2022). Integration Of Advanced NDT Techniques & Implementing QA/QC Programs In Enhancing Safety And Integrity In Oil & Gas Operations. *American Journal of Interdisciplinary Studies*, *3*(02), 01-35. https://doi.org/10.63125/9pzxgq74

[140] Roksana, H. (2023). Automation In Manufacturing: A Systematic Review Of Advanced Time Management Techniques To Boost Productivity. *American Journal of Scholarly Research and Innovation*, *2*(01), 50-78. https://doi.org/10.63125/z1wmcm42

[141] Roksana, H., Ammar, B., Noor Alam, S., & Ishtiaque, A. (2024). Predictive Maintenance in Industrial Automation: A Systematic Review Of IOT Sensor Technologies And AI Algorithms. *American Journal of Interdisciplinary Studies*, *5*(01), 01-30. https://doi.org/10.63125/hd2ac988

[142] Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, *2*(2), 121-135. https://doi.org/10.1093/cybsec/tyw001

[143] Roshanaei, M. (2021). Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies. *Journal of Computer and Communications*, *09*(08), 80-102. https://doi.org/10.4236/jcc.2021.98006

[144] Roy, P. P., Abdullah, M. S., & Sunny, M. A. U. (2024). Revolutionizing Structural Engineering: Innovations in Sustainable Design and Construction. *European Journal of Advances in Engineering and Technology*, *11*(5), 94-99.

[145] Sabid, A. M., & Kamrul, H. M. (2024). Computational And Theoretical Analysis On The Single Proton Transfer Process In Adenine Base By Using DFT Theory And Thermodynamics. *IOSR Journal of Applied Chemistry*.

[146] Schmidhuber, J. (2014). Deep learning in neural networks. *Neural networks : the official journal of the International Neural Network Society*, *61*(NA), 85-117. https://doi.org/10.1016/j.neunet.2014.09.003

[147] Schmidt, P. J., Wood, J. T., & Grabski, S. V. (2016). Business in the Cloud: Research Questions on Governance, Audit, and Assurance. *Journal of Information Systems*, *30*(3), 173-189. https://doi.org/10.2308/isys-51494

[148] Shahan, A., Anisur, R., & Md, A. (2023). A Systematic Review Of AI And Machine Learning-Driven IT Support Systems: Enhancing Efficiency And Automation In Technical Service Management. *American Journal of Scholarly Research and Innovation*, *2*(02), 75-101. https://doi.org/10.63125/fd34sr03

[149] Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, *124*, 102974-102974. https://doi.org/10.1016/j.cose.2022.102974

[150] Sharif, K. S., Uddin, M. M., & Abubakkar, M. (2024, 17-19 Dec. 2024). NeuroSignal Precision: A Hierarchical Approach for Enhanced Insights in Parkinson's Disease Classification. 2024 International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA),

[151] Shofiullah, S., Shamim, C. M. A. H., Islam, M. M., & Sumi, S. S. (2024). Comparative Analysis Of Cost And Benefits Between Renewable And Non-Renewable Energy Projects: Capitalizing Engineering Management For Strategic Optimization. *Academic Journal On Science, Technology, Engineering & Mathematics Education*, *4*(03), 103-112. https://doi.org/10.69593/ajsteme.v4i03.100

[152] Shohel, M. S. H., Islam, M. M., Prodhan, R. K., & Morshed, A. S. M. (2024). Lifecycle Management Of Renewable Energy Systems In Residential Housing Construction. *Frontiers in Applied Engineering and Technology*, *1*(01), 124-138. https://doi.org/10.70937/faet.v1i01.23

[153] Shu, X., Zhang, J., Yao, D. D., & Feng, W.-c. (2016). Fast Detection of Transformed Data Leaks. *IEEE Transactions on Information Forensics and Security*, *11*(3), 528-542. https://doi.org/10.1109/tifs.2015.2503271

[154] Siponen, M. T., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, *46*(5), 267-270. https://doi.org/10.1016/j.im.2008.12.007

[155] Smith, T. J., Higgs, J. L., & Pinsker, R. E. (2018). Do Auditors Price Breach Risk in Their Audit Fees. *Social Science Research Network*, *NA*(NA), NA-NA. https://doi.org/NA

[156] Snyder, D., Powers, J. D., Bodine-Baron, E., Fox, B., Kendrick, L., & Powell, M. H. (2015). *Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles* (Vol. NA). NA. https://doi.org/NA

[157] Sohel, A., Alam, M. A., Hossain, A., Mahmud, S., & Akter, S. (2022). Artificial Intelligence In Predictive Analytics For Next-Generation Cancer Treatment: A Systematic Literature Review Of Healthcare Innovations In The USA. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *1*(01), 62-87. https://doi.org/10.62304/jieet.v1i01.229

[158] Somani, U., Lakhani, K., & Mundra, M. (2010). Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing. *2010 First International Conference On Parallel, Distributed and Grid Computing (PDGC 2010)*, *NA*(NA), 211-216. https://doi.org/10.1109/pdgc.2010.5679895

[159] Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach. *International Journal of Information Management*, *36*(2), 215-225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

[160] Stahl, B. C., Doherty, N. F., & Shaw, M. C. (2011). Information security policies in the UK Healthcare Sector: A critical evaluation. *Information Systems Journal*, *22*(1), 77-94. https://doi.org/10.1111/j.1365-2575.2011.00378.x

[161] Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2013). Information Security Professionals' Perceptions about the Relationship between the Information Security and Internal Audit Functions. *Journal of Information Systems*, *27*(2), 65-86. https://doi.org/10.2308/isys-50510

[162] Subashini, S., & Kavitha, V. (2011). Review: A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1-11. https://doi.org/10.1016/j.jnca.2010.07.006

[163] Subramanian, D. V., & Kumar, K. P. (2016). Fuzzy based modeling for an effective IT security policy management. *2016 SAI Computing Conference (SAI)*, *NA*(NA), 173-181. https://doi.org/10.1109/sai.2016.7555979

[164] Sun, L., Srivastava, R. P., & Mock, T. J. (2006). An Information Systems Security Risk Assessment Model Under the Dempster-Shafer Theory of Belief Functions. *Journal of Management Information Systems*, *22*(4), 109-142. https://doi.org/10.2753/mis0742-1222220405

[165] Sun, P. (2020). Security and privacy protection in cloud computing: Discussions and challenges. *Journal of Network and Computer Applications*, *160*(NA), 102642-NA. https://doi.org/10.1016/j.jnca.2020.102642

[166] Sunny, M. A. U. (2024a). Eco-Friendly Approach: Affordable Bio-Crude Isolation from Faecal Sludge Liquefied Product. *Journal of Scientific and Engineering Research*, *11*(5), 18-25.

[167] Sunny, M. A. U. (2024b). Effects of Recycled Aggregate on the Mechanical Properties and Durability of Concrete: A Comparative Study. *Journal of Civil and Construction Engineering*, 7-14.

[168] Sunny, M. A. U. (2024c). Unveiling spatial insights: navigating the parameters of dynamic Geographic Information Systems (GIS) analysis. *International Journal of Science and Research Archive*, *11*(2), 1976-1985.

[169] Süzen, A. A. (2020). A Risk-Assessment of Cyber Attacks and Defense Strategies in Industry 4.0 Ecosystem. *International Journal of Computer Network and Information Security*, *12*(1), 1-12. https://doi.org/10.5815/ijcnis.2020.01.01

[170] Szádeczky, T. (2018). Cybersecurity Authorities and Related Policies in the EU and Hungary. *Central and Eastern European eDem and eGov Days*, *331*(NA), 287-299. https://doi.org/10.24989/ocg.v331.24

[171] Talib, A. M., & Alomary, F. O. (2016). ICC 2016 - Cloud Computing Based E-Commerce as a Service Model: Impacts and Recommendations. *Proceedings of the International Conference on Internet of things and Cloud Computing*, *NA*(NA), 27-27. https://doi.org/10.1145/2896387.2896412

[172] Tamburri, D. A. (2020). Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation. *Information Systems*, *91*(NA), 101469-NA. https://doi.org/10.1016/j.is.2019.101469

[173] Tchernykh, A., Schwiegelsohn, U., Talbi, E.-G., & Babenko, M. (2019). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of Computational Science*, *36*(NA), 100581-NA. https://doi.org/10.1016/j.jocs.2016.11.011

[174] Ter, K. L. (2018). Singapore's cybersecurity strategy. *Computer Law & Security Review*, *34*(4), 924-927. https://doi.org/10.1016/j.clsr.2018.05.001

[175] Thapa, C., & Camtepe, S. (2020). Precision health data: Requirements, challenges and existing techniques for data security and privacy. *Computers in biology and medicine*, *129*(NA), 104130-NA. https://doi.org/10.1016/j.compbiomed.2020.104130

[176] Tinoco, M. H., & Wilson, N. (2013). Financial distress and bankruptcy prediction among listed companies using accounting, market and macroeconomic variables. *International Review of Financial Analysis*, *30*(NA), 394-419. https://doi.org/10.1016/j.irfa.2013.02.013

[177] Tissir, N., Kafhali, S. E., & Aboutabit, N. (2020). Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal. *Journal of Reliable Intelligent Environments*, *7*(2), 69-84. https://doi.org/10.1007/s40860-020-00115-0

[178] Tonoy, A. A. R. (2022). Mechanical Properties and Structural Stability of Semiconducting Electrides: Insights For Material. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *1*(01), 18-35. https://doi.org/10.62304/jieet.v1i01.225

[179] Tonoy, A. A. R., & Khan, M. R. (2023). The Role of Semiconducting Electrides In Mechanical Energy Conversion And Piezoelectric Applications: A Systematic Literature Review. *American Journal of Scholarly Research and Innovation*, *2*(1), 01-23. https://doi.org/10.63125/patvqr38

[180] Tsesis, A. (2019). Data Subjects' Privacy Rights: Regulation of Personal Data Retention and Erasure. *SSRN Electronic Journal*, *NA*(NA), NA-NA. https://doi.org/10.2139/ssrn.3325973

[181] Uddin Shipu, I., Bhowmick, D., & Lal Dey, N. (2024). Development and applications of flexible piezoelectric nanogenerators using BaTiO3, PDMS, and MWCNTs for energy harvesting and sensory integration in smart systems. *International Journal of Scientific and Research Publications*, *14*(6), 221.

[182] Ulven, J. B., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet*, *13*(2), 39-NA. https://doi.org/10.3390/fi13020039

[183] Vasarhelyi, M. A. (2012). Financial Accounting Standards Should Not Matter: It's Just a Layer. *Journal of Information Systems*, *26*(2), 1-11. https://doi.org/10.2308/isys-10316

[184] Vincent, N. E., Higgs, J. L., & Pinsker, R. E. (2018). Board and Management-Level Factors Affecting the Maturity of IT Risk Management Practices. *Journal of Information Systems*, *33*(3), 117-135. https://doi.org/10.2308/isys-52229

[185] Walton, S., Wheeler, P. R., Zhang, Y., & Zhao, X. R. (2020). An Integrative Review and Analysis of Cybersecurity Research: Current State and Future Directions. *Journal of Information Systems*, *35*(1), 155-186. https://doi.org/10.2308/isys-19-033

[186] Wang, J., Gupta, M., & Rao, H. R. (2015). Insider threats in a financial institution: analysis of attack-proneness of information systems applications. *MIS Quarterly*, *39*(1), 91-112. https://doi.org/10.25300/misq/2015/39.1.05

[187] Wangen, G., Hallstensen, C., & Snekkenes, E. (2017). A framework for estimating information security risk assessment method completeness. *International Journal of Information Security*, *17*(6), 681-699. https://doi.org/10.1007/s10207-017-0382-0

[188] Westland, J. C. (2020). The information content of Sarbanes-Oxley in predicting security breaches. *Computers & Security*, *90*(NA), 101687-NA. https://doi.org/10.1016/j.cose.2019.101687

[189] Wu, C.-H., & Irwin, J. D. (2016). *Introduction to Computer Networks and Cybersecurity* (Vol. NA). CRC Press. https://doi.org/10.1201/9781466572140

[190] Yang, P., Xiong, N., & Ren, J. (2020). Data Security and Privacy Protection for Cloud Storage: A Survey. *IEEE Access*, *8*(NA), 131723-131740. https://doi.org/10.1109/access.2020.3009876

[191] Yar, M. (2005). The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), 407-427. https://doi.org/10.1177/147737080556056

[192] Younus, M. (2022). Reducing Carbon Emissions in The Fashion And Textile Industry Through Sustainable Practices and Recycling: A Path Towards A Circular, Low-Carbon Future. *Global Mainstream Journal of Business, Economics, Development & Project Management*, *1*(1), 57-76. https://doi.org/10.62304/jbedpm.v1i1.226

[193] Zhao, X., Xue, L., & Whinston, A. B. (2013). Managing Interdependent Information Security Risks: Cyberinsurance, Managed Security Services, and Risk Pooling Arrangements. *Journal of Management Information Systems*, *30*(1), 123-152. https://doi.org/10.2753/mis0742-1222300104

[194] Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583-592. https://doi.org/10.1016/j.future.2010.12.006