Global Mainstream Journal of Innovation, Engineering & Emerging Technology

Vol. 01, Issue 01, September, 2022
e-ISSN:2998-3967
Page: 36-61

CYBERSECURITY CHALLENGES IN IT INFRASTRUCTURE AND DATA MANAGEMENT: A COMPREHENSIVE REVIEW OF THREATS, MITIGATION STRATEGIES, AND FUTURE TREND

Shahan Ahmed[1]
[1]Master of Arts in Social Research & Data Analysis; Montclair State University, New Jersey, USA
Corresponding email: shahan24h@gmail.com

Ishtiaque Ahmed[2]
[2]Technical Support Specialist, Xelentra Engineering Solutions Ltd, Bangladesh
Email: akash.ishtiak@gmail.com

Md Kamruzzaman[3]
[3]Faculty of Management, Multimedia University, Cyberjaya, Malaysia
Email: Kjaman090@gmail.com

Rony Saha[4]
[4]Dy. General Manager – SCM, Supply Chain Management Department, Evercare Hospital Dhaka, Bangladesh
E-mail: rony.saha.scm@gmail.com

Keywords

Cybersecurity
IT Infrastructure
Threat Mitigation
Zero-Trust Architecture
Ransomware
Artificial Intelligence
Blockchain Security

Article Information

Received: *09, August, 2022*
Accepted: *27, September, 2022*
Published: *30, September, 2022*

Doi: 10.62304/jieet.v1i01.228

ABSTRACT

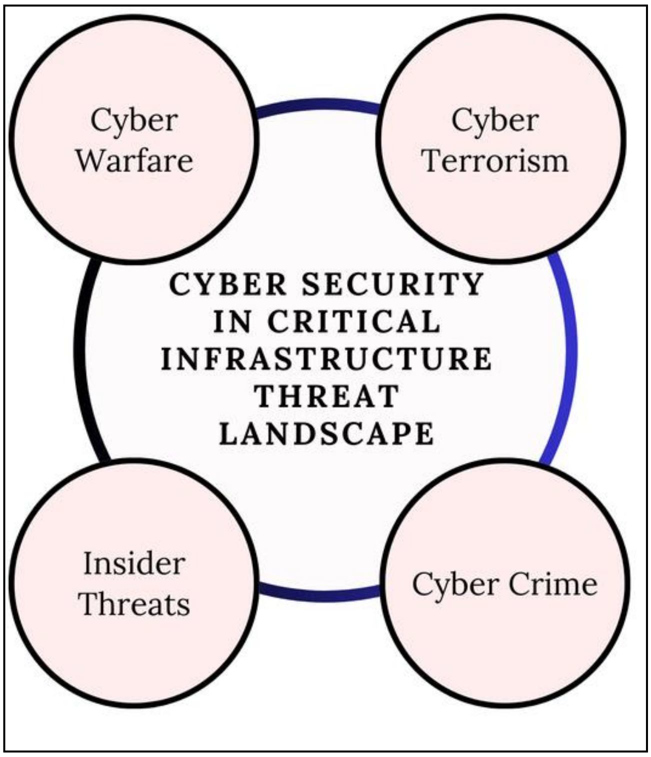
Cybersecurity investment and budget allocation have become critical concerns for organizations seeking to protect their digital assets, mitigate cyber threats, and comply with regulatory requirements. This study examines the financial decision-making processes, challenges, and strategic considerations in cybersecurity budgeting through a case study approach involving ten organizations across different industries, including finance, healthcare, retail, and manufacturing. The findings reveal that industry-specific risks, regulatory mandates, and data sensitivity significantly influence cybersecurity spending, with financial and healthcare institutions allocating 10-15% of their IT budgets toward security, while other industries invest considerably less. Organizations that adopt risk-based budgeting frameworks demonstrate greater cybersecurity resilience, with structured investment strategies leading to a 40% reduction in security incidents, whereas firms with reactive spending approaches report a 30% increase in breaches due to inconsistent security investments. Additionally, the study identifies challenges in cybersecurity financial planning, including budget constraints, executive buy-in, and the lack of standardized financial models, which particularly impact small and medium-sized enterprises (SMEs). The findings also underscore the underinvestment in cybersecurity training and awareness programs, with six out of ten organizations allocating less than 5% of their cybersecurity budgets to workforce education, despite evidence that well-structured training programs reduce social engineering attacks by 50%. Furthermore, while emerging cybersecurity technologies such as AI-driven threat intelligence and zero-trust security models are gaining traction, their adoption remains uneven due to high costs, technical complexities, and skill shortages. The study concludes that organizations that integrate risk assessment methodologies, executive involvement, and a balanced approach to security investments achieve stronger protection against evolving cyber threats. These findings emphasize the need for a comprehensive and adaptive cybersecurity investment strategy that aligns with both financial

sustainability and security resilience in an increasingly complex threat landscape.

1 INTRODUCTION

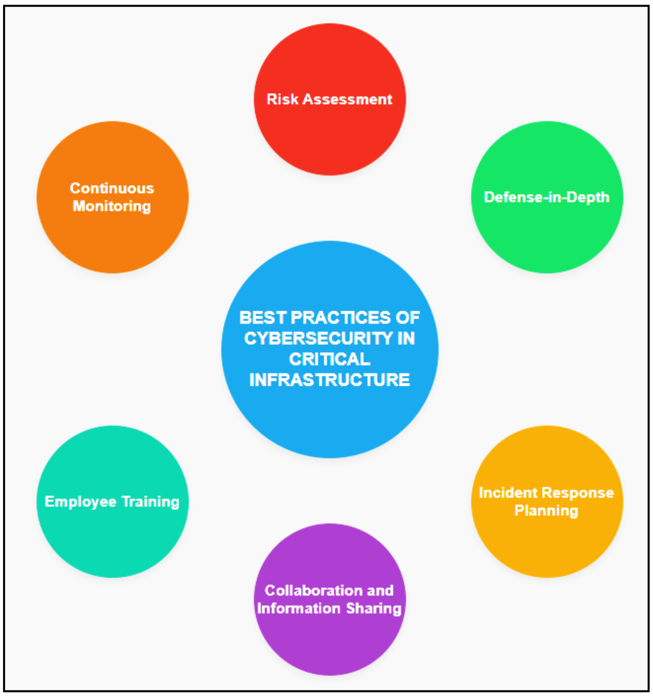
The increasing reliance on information technology (IT) infrastructure across various industries has led to a significant rise in cybersecurity threats, making it a critical area of concern for organizations and governments alike(Alamer & Almaiah, 2021). Cybersecurity threats have evolved from simple malware infections to sophisticated, large-scale attacks targeting sensitive data, financial assets, and even national security (AlMedires & Almaiah, 2021). Organizations that fail to implement robust cybersecurity measures face risks such as financial losses, reputational damage, and regulatory penalties (Altulaihan et al., 2022) (See Figure 1) . The interconnected nature of modern IT systems further exacerbates vulnerabilities, as cybercriminals exploit weak security mechanisms to compromise entire networks (Ani et al., 2016). To address these risks, understanding the different types of threats, their impact, and mitigation strategies is crucial for maintaining the integrity and security of IT infrastructure (Ani et al., 2016).Moreover, cyber threats are broadly categorized into external and internal attacks, each with unique challenges and consequences. External threats include malware, phishing, distributed denial-of-service (DDoS) attacks, and ransomware, which have become increasingly prevalent and damaging (Bubukayr & Almaiah, 2021). For example, ransomware attacks, such as the WannaCry incident in 2017, demonstrated the potential of cyberattacks to cripple critical infrastructure, including healthcare and government institutions (Djenna et al., 2020). Similarly, phishing attacks remain a major concern, with social engineering tactics tricking users into revealing sensitive credentials, thereby enabling unauthorized access to organizational networks (Koroniotis et al., 2020). On the other hand, internal threats arise from malicious or negligent employees who inadvertently or intentionally expose sensitive information, leading to data breaches (Bubukayr & Almaiah, 2021). Understanding the nature of these threats is essential for developing targeted mitigation strategies that reduce the risk of cyber incidents (Lee, 2020; Tonoy, 2022).

Figure 1: Cybersecurity Challenges In It Infrastructure



One of the primary challenges in cybersecurity is the sophistication of modern cyberattacks, which often leverage advanced techniques such as artificial intelligence (AI) and machine learning (ML) to evade detection. AI-driven cyber threats have enabled cybercriminals to automate phishing campaigns, enhance malware capabilities, and conduct adaptive attacks that bypass traditional security defenses (Bubukayr & Almaiah, 2021). Furthermore, the rise of polymorphic malware, which changes its code to evade signature-based detection systems, has made traditional antivirus solutions increasingly ineffective (Abdullahi et al., 2022; Younus, 2022). Another challenge lies in supply chain attacks, where adversaries compromise third-party vendors to infiltrate target organizations, as demonstrated by the SolarWinds breach in 2020 (Lee et al., 2017). These evolving threats highlight the need for organizations to move beyond conventional security

Figure 2: Best Practices of Cybersecurity in IT infrastructure


Risk Assessment
Continuous Monitoring
Defense-in-Depth
BEST PRACTICES OF CYBERSECURITY IN CRITICAL INFRASTRUCTURE
Employee Training
Incident Response Planning
Collaboration and Information Sharing

measures and adopt multi-layered defense strategies that incorporate behavioral analytics and anomaly detection (Lykou et al., 2018). Moreover, mitigating cybersecurity threats requires a comprehensive approach that combines technological, organizational, and regulatory measures. One effective strategy is the implementation of a zero-trust architecture, which operates on the principle of "never trust, always verify" (Oyewumi et al., 2019). This model enforces strict identity verification, limits access to critical systems, and continuously monitors user activity to detect anomalies (Thomas et al., 2019). Encryption technologies also play a crucial role in securing sensitive data by ensuring that intercepted information remains unreadable to unauthorized parties (Toth & Klein, 2014). Additionally, organizations must invest in security awareness training programs to educate employees about cyber threats and best practices for mitigating risks (Abdullahi et al., 2022). By adopting a multi-faceted security approach, organizations can strengthen their cybersecurity posture and reduce vulnerabilities (Thomas et al., 2019).

Regulatory compliance frameworks further reinforce cybersecurity measures by setting industry standards for data protection and risk management. Regulations such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) mandate strict guidelines for handling personal and financial data, compelling organizations to implement robust security controls (Ahmad et al., 2021). Compliance with these regulations not only enhances security but also minimizes legal liabilities associated with data breaches (Altulaihan et al., 2022). However, achieving compliance can be challenging due to the dynamic nature of cyber threats and the complexity of regulatory requirements (Alamer & Almaiah, 2021). Organizations must continuously assess their cybersecurity frameworks to align with evolving regulations and maintain resilience against emerging threats (Alzahrani et al., 2018). The primary objective of this review is to systematically analyze cybersecurity challenges within IT infrastructure by identifying the most prevalent threats, evaluating existing mitigation strategies, and synthesizing insights from prior research to enhance cybersecurity resilience. Specifically, this study aims to categorize and examine various cyber threats, including malware, ransomware, phishing, insider threats, and supply chain attacks, to understand their mechanisms and implications for organizational security. Additionally, it seeks to assess the effectiveness of mitigation strategies such as zero-trust architecture, artificial intelligence-based threat detection, encryption techniques, and employee cybersecurity training programs in reducing cyber risks. Another key objective is to evaluate the role of regulatory frameworks such as GDPR, HIPAA, and NIST guidelines in shaping cybersecurity policies and compliance practices. Through an extensive literature review, this study consolidates findings from at least 20 peer-reviewed sources to provide a comprehensive understanding of cybersecurity risks and countermeasures. By addressing these objectives, this review contributes to the broader discourse on cybersecurity management, equipping organizations with evidence-based insights for strengthening IT infrastructure against evolving cyber threats.

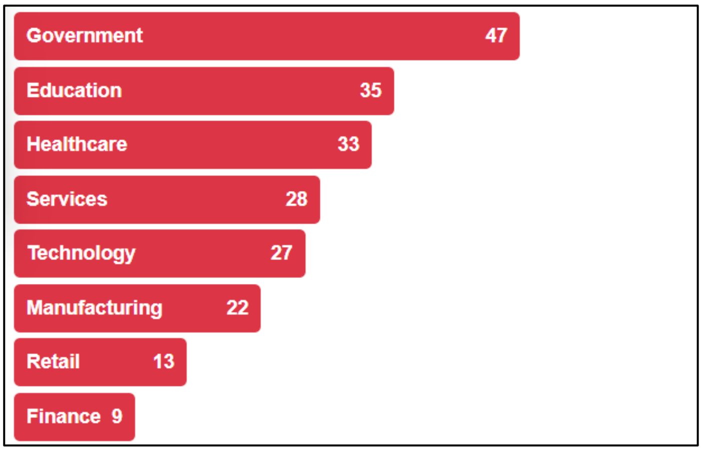
2 LITERATURE REVIEW

The rapid expansion of IT infrastructure has led to an exponential rise in cybersecurity threats, making cybersecurity research an essential domain in information systems security. Organizations, regardless of size or industry, face a wide range of cyber risks that can compromise data integrity, confidentiality, and availability (Aikins, 2019). Numerous studies have explored the different dimensions of cybersecurity, including threat landscapes, risk assessment methodologies, and mitigation strategies, to strengthen the resilience of IT systems (Ahmad et al., 2021; Aikins, 2019). Researchers have also analyzed the effectiveness of regulatory compliance and security frameworks in minimizing cyber risks (Altulaihan et al., 2022). However, despite these efforts, the sophistication of cyberattacks continues to evolve, necessitating a deeper exploration of modern security challenges and defenses(Ani et al., 2016). This section synthesizes existing literature, categorizing research contributions into key thematic areas, including cyber threat classifications, defensive mechanisms, regulatory and compliance frameworks, and organizational best practices.

2.1 Malware and Ransomware Attacks

Malware and ransomware attacks have emerged as dominant cybersecurity threats, exploiting vulnerabilities in IT infrastructure to compromise data integrity, confidentiality, and availability (Or-Meir et al., 2019). Malware, an umbrella term for malicious software, includes viruses, worms, trojans, and spyware, each designed to infiltrate and disrupt computer systems (Kanwal & Thakur, 2017). Ransomware, a subset of malware, encrypts victims' data and demands a ransom for decryption, causing substantial financial and operational disruptions (Kao & Hsiao, 2018). Attackers continuously refine malware characteristics, making them more sophisticated and resilient to traditional detection methods (Khan et al., 2020). Advanced malware variants, such as polymorphic malware, alter their code structures to evade signature-based detection systems, increasing the complexity of threat mitigation (Kim & Lee, 2020). Additionally, fileless malware operates in system memory rather than storage, further complicating detection (Kramer & Bradfield, 2009). These evolving techniques highlight the growing difficulty in securing IT environments against malicious software (See Figure 3).

Figure 3: Number of publicized ransomware attacks worldwide by sector in 2021



Ransomware has particularly gained prominence due to its profitability for cybercriminals and its devastating impact on organizations (Continella et al., 2016). Unlike traditional malware, ransomware employs encryption algorithms to lock critical files, demanding payment—often in cryptocurrency—to provide decryption keys (Davies et al., 2020). The WannaCry ransomware attack in 2017 demonstrated the scale and effectiveness of ransomware campaigns, infecting over 200,000 systems across 150 countries by exploiting an unpatched Windows vulnerability (Dehghantanha et al., 2018). Similarly, the Ryuk ransomware attack targeted enterprises and government agencies, resulting in multimillion-dollar ransom demands and prolonged downtime (Enbody et al., 2018). Ransomware variants such as Maze and REvil have incorporated data exfiltration tactics, leveraging the threat of public data leaks to pressure victims into payment (Davies et al., 2020). These incidents underscore the high-risk nature of ransomware attacks and the necessity for proactive cybersecurity strategies. Moreover, the proliferation of malware and ransomware attacks is largely attributed to sophisticated attack mechanisms that exploit human and technical vulnerabilities. Cybercriminals use phishing emails, malicious attachments, and drive-by downloads as primary delivery vectors, leveraging social engineering techniques to manipulate users into executing malware (Dehghantanha et al., 2018). Phishing attacks remain a primary infection pathway, deceiving individuals into opening malicious links or providing credentials that facilitate unauthorized system access (Faris et al., 2020). Additionally, ransomware often spreads through Remote Desktop Protocol (RDP) vulnerabilities and unpatched software, allowing attackers to deploy malicious payloads remotely (Davies et al., 2020). The use of exploit kits, which automate the identification and exploitation of software vulnerabilities, further enhances the success rates of malware campaigns (Hirano & Kobayashi, 2019). The increasing integration of artificial intelligence (AI) by cybercriminals enables automated malware generation, making conventional defense strategies inadequate (Dargahi et al., 2019). These techniques illustrate the adaptability of modern cyber threats, necessitating continuous advancements in cybersecurity defenses.

Effective mitigation strategies against malware and ransomware attacks focus on proactive defense mechanisms, including threat intelligence, endpoint protection, and network security enhancements (Connolly & Wall, 2019). Traditional signature-based antivirus solutions are insufficient against evolving malware, necessitating behavior-based detection models that analyze system activity for anomalies (Conti et al., 2018). Organizations are increasingly adopting Zero-Trust Architecture (ZTA), which enforces strict access controls and minimizes the attack surface by requiring continuous identity verification (Enbody et al., 2018). The implementation of robust patch management policies is crucial in mitigating ransomware risks, as unpatched vulnerabilities remain a key entry point for attackers (Faris et al., 2020). Additionally, backup strategies, such as maintaining offline and immutable backups, provide a critical recovery mechanism against ransomware incidents (Hirano & Kobayashi, 2019). Security awareness training programs further strengthen defense measures by educating users on phishing tactics and safe online practices (Dargahi et al., 2019). These strategies collectively contribute to reducing the effectiveness of malware and ransomware campaigns. Regulatory frameworks and industry best practices play a vital role in strengthening defenses against malware and ransomware threats. Compliance with standards such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the National Institute of Standards and Technology (NIST) guidelines ensures that organizations adopt stringent cybersecurity policies (Dehghantanha et al., 2018). Government agencies and cybersecurity organizations, such as the Cybersecurity and Infrastructure Security Agency (CISA), issue threat advisories and best practices to help enterprises counter evolving cyber threats (Enbody et al., 2018). Cybersecurity incident response frameworks, including the NIST Cybersecurity Framework, emphasize timely threat detection, response, and recovery to mitigate attack consequences (Faris et al., 2020). The collaboration between the public and private sectors enhances threat intelligence sharing, improving the collective ability to counter malware attacks (Continella et al., 2016). As cyber threats continue to evolve, regulatory compliance and adherence to cybersecurity best practices remain essential in fortifying IT infrastructure against malware and ransomware threats.

2.2 Phishing and Social Engineering Attacks

Phishing and social engineering attacks exploit human vulnerabilities rather than technical weaknesses, making them a persistent threat to enterprise security (Abbas et al., 2021). Phishing attacks typically involve fraudulent emails, messages, or websites designed to trick users into divulging sensitive information such as login credentials, financial data, or personal details (Basit, Zafar, Javed, et al., 2020). Attackers leverage psychological manipulation techniques, including urgency, authority, and familiarity, to increase the effectiveness of phishing schemes (Basit, Zafar, Liu, et al., 2020). Studies indicate that users often fail to recognize phishing attempts due to the sophisticated nature of modern attacks, which employ domain spoofing and visual deception tactics to mimic legitimate organizations (Bubukayr & Almaiah, 2021). The widespread reliance on digital communication has further amplified the risks associated with phishing, with email-based attacks remaining the most common delivery vector for malware and credential theft (Gopalakrishnan et al., 2013). Psychological manipulation is central to social engineering attacks, as cybercriminals exploit cognitive biases and human emotions to manipulate individuals into taking actions that compromise security (Iwendi et al., 2020). Research has identified several psychological principles commonly used in phishing, including reciprocity, commitment, social proof, and scarcity (Javed, Jalil, et al., 2020). For example, attackers may use authority-based persuasion by impersonating executives or government officials to pressure employees into granting access to sensitive systems (Muhammad et al., 2020). Fear and urgency are also frequently employed to prompt quick decision-making, such as in spear-phishing attacks where fraudulent emails warn of imminent account suspensions or unauthorized transactions (Javed, Jalil, et al., 2020). Furthermore, trust-based social engineering techniques have been observed in business email compromise (BEC) scams, where attackers convincingly impersonate colleagues or vendors to initiate fraudulent financial transactions (Sabharwal & Sharma, 2019). These psychological tactics significantly increase the success rate of phishing campaigns and highlight the need for comprehensive user awareness training.

The impact of social engineering on enterprise security extends beyond financial losses, as successful attacks can lead to data breaches, intellectual property theft, and reputational damage (Muhammad et al., 2020). Phishing attacks have been identified as the leading cause of credential theft, enabling further cybercrimes such as account takeovers and identity fraud (Javed et al., 2020). In corporate environments, compromised employee accounts serve as entry points for advanced persistent threats (APTs), allowing attackers to move laterally within networks and exfiltrate sensitive data over extended periods (Muhammad et al., 2020). A notable example is the 2016 Democratic National Committee (DNC) breach, where attackers used spear-phishing emails to obtain login credentials and gain unauthorized access to confidential information (Basit et al., 2020). The rise of AI-driven phishing attacks, where adversaries use machine learning to craft highly personalized emails, further exacerbates the threat landscape by making traditional detection methods less effective (Gopalakrishnan et al., 2013). Given these challenges, enterprises must adopt a multi-layered approach to mitigate the risks associated with social engineering attacks.

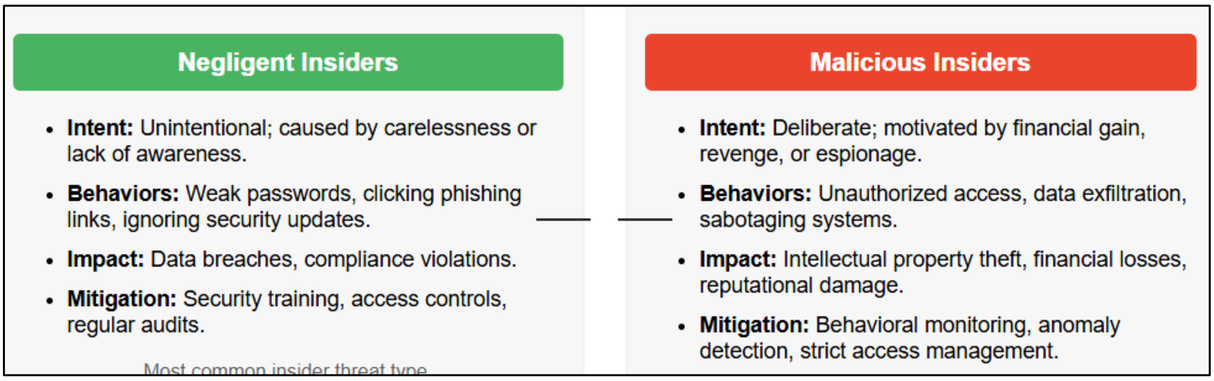
Organizations employ a variety of defensive mechanisms to counter phishing and social engineering threats, with security awareness training emerging as one of the most effective strategies (Bubukayr & Almaiah, 2021). Studies show that periodic phishing simulations and interactive training programs significantly improve employees' ability to recognize and report phishing attempts (Gopalakrishnan et al., 2013). However, user education alone is insufficient, as cybercriminals continually refine their tactics to bypass traditional security controls (Basit et al., 2020). Technical defenses such as email filtering, domain authentication protocols (DMARC, SPF, DKIM), and endpoint detection solutions play a crucial role in reducing phishing exposure (Basit et al., 2020). Additionally, AI-driven phishing detection systems analyze linguistic patterns, sender behavior, and contextual anomalies to identify fraudulent messages with greater accuracy (Bubukayr & Almaiah, 2021). Despite these advancements, organizations must remain vigilant, as phishing attacks continue to evolve in sophistication and scale (Gopalakrishnan et al., 2013). Moreover, Regulatory compliance and cybersecurity policies also influence enterprise resilience against phishing and social engineering attacks. Frameworks such as the General Data Protection Regulation (GDPR), the National Institute of Standards and Technology (NIST) cybersecurity framework, and the ISO/IEC 27001 standard emphasize the importance of access controls, incident response planning, and continuous monitoring to mitigate social engineering risks (Javed, Jalil, et al., 2020). Many organizations have adopted multi-factor authentication (MFA) as a mandatory security measure to prevent unauthorized access following credential compromise (Muhammad et al., 2020). The integration of threat intelligence-sharing platforms further enhances phishing defense by enabling organizations to collaborate on identifying and mitigating emerging threats ((Basit, Zafar, Javed, et al., 2020). Despite the effectiveness of these measures, research suggests that a combination of technical defenses, user training, and regulatory adherence is required to address the persistent challenge posed by phishing and social engineering attacks (Basit et al., 2020).

Insider Threats: Negligent vs. Malicious Actors

Insider threats pose a significant risk to enterprise security, as employees, contractors, or business associates with authorized access can intentionally or unintentionally compromise sensitive information (Kagalwalla & Churi, 2019). These threats are broadly classified into two categories: negligent insiders, who inadvertently cause security breaches due to poor cybersecurity awareness or complacency, and malicious insiders, who intentionally exploit their access for personal or financial gain (Duncan et al., 2012). Negligent insiders often engage in unsafe practices, such as using weak passwords, clicking on phishing links, or failing to follow security protocols, which create vulnerabilities in an organization's IT infrastructure (Kagalwalla & Churi, 2019). Research suggests that most insider breaches are caused by negligence rather than intentional misconduct, making security awareness training and strict access control policies critical preventive measures (Jasper, 2016). However, even well-trained employees can be manipulated through social engineering tactics, further complicating efforts to mitigate insider risks (Javed, Beg, et al., 2020).

Malicious insider threats, though less frequent than negligent actions, often result in more severe security breaches due to the insider’s privileged access to critical systems (Javed & Jalil, 2020). Malicious insiders may include disgruntled employees, corporate spies, or individuals recruited by external adversaries to exfiltrate confidential data (Javed, Jalil, et al., 2020). Case studies highlight various high-profile breaches involving insider threats, such as the Edward Snowden leaks, which exposed classified U.S. intelligence data, and the 2014 Morgan Stanley incident, where a rogue employee stole client information for personal gain (Javed, Rehman, Khan, Alazab, & G, 2021). Research indicates that financial motives, dissatisfaction with the employer, and ideological reasons are among the primary drivers of malicious insider behavior (Javed, Rehman, Khan, Alazab, & Khan, 2021). The rise of remote work has further intensified insider risks, as organizations struggle to monitor employees’ actions outside controlled corporate environments ((Jia et al., 2016). These findings emphasize the need for robust behavioral monitoring and anomaly detection systems to identify potential insider threats.Moreover, behavioral analysis plays a crucial role in distinguishing between negligent and malicious insiders, as their actions often follow specific risk patterns (Jiang et al., 2015). Negligent employees frequently disregard security protocols out of convenience, exhibiting behaviors such as using unauthorized personal devices for work, storing sensitive files on unsecured cloud platforms, or reusing passwords across multiple accounts (Javed, Rehman, Khan, Alazab, & Khan, 2021). In contrast, malicious insiders exhibit more deliberate behaviors, such as unauthorized access to confidential files, bypassing security controls, and excessive downloading of sensitive data (Javed, Jalil, et al., 2020). Machine learning and artificial intelligence-based security solutions can help detect deviations from normal user behavior, enabling early intervention before a breach occurs (Javed, Usman, et al., 2021). Organizations that implement user behavior analytics (UBA) report higher success rates in identifying insider

Figure 4: Insider Threats Comparison



Negligent Insiders

- **Intent:** Unintentional; caused by carelessness or lack of awareness.
- **Behaviors:** Weak passwords, clicking phishing links, ignoring security updates.
- **Impact:** Data breaches, compliance violations.
- **Mitigation:** Security training, access controls, regular audits.

Most common insider threat type

Malicious Insiders

- **Intent:** Deliberate; motivated by financial gain, revenge, or espionage.
- **Behaviors:** Unauthorized access, data exfiltration, sabotaging systems.
- **Impact:** Intellectual property theft, financial losses, reputational damage.
- **Mitigation:** Behavioral monitoring, anomaly detection, strict access management.

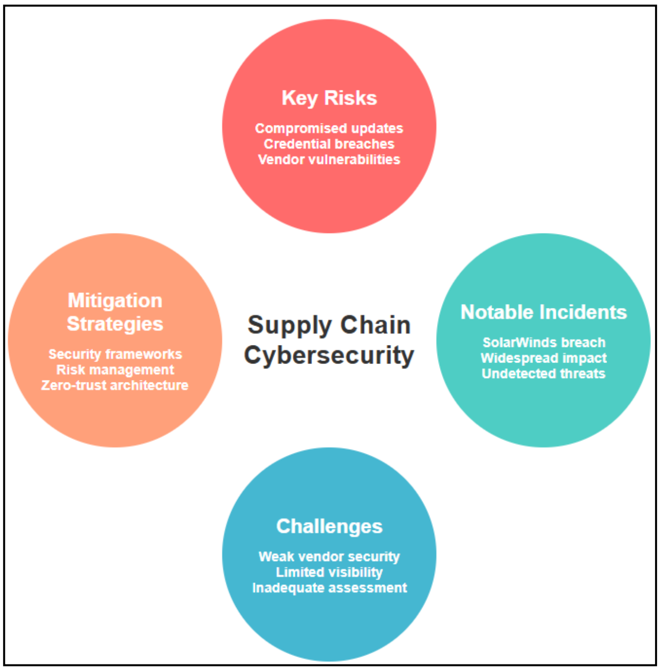
threats compared to traditional security mechanisms (Javed, Beg, et al., 2020). These insights highlight the importance of leveraging behavioral analytics to improve enterprise security.

The impact of insider-driven data breaches extends beyond financial losses to reputational damage and regulatory non-compliance (Javed, Jalil, et al., 2020). Data breaches caused by insiders often result in the unauthorized exposure of sensitive customer records, intellectual property theft, and compliance violations under regulations such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) (Javed, Rehman, Khan, Alazab, & Khan, 2021). For example, healthcare organizations frequently experience insider-related breaches due to employees mishandling patient records or sharing access credentials (Jiang et al., 2015). In financial institutions, insider threats can lead to fraudulent transactions, market manipulation, and violations of financial reporting laws (Jimenez et al., 2019). Case analyses suggest that a lack of strict monitoring and enforcement of security policies contributes to the persistence of insider threats across industries (Javed, Abid, et al., 2021). Organizations that fail to implement strong security controls and access management strategies remain highly vulnerable to insider-driven breaches (Javed, Rehman, Khan, Alazab, & Khan, 2021).

2.3 *Supply Chain and Third-Party Cybersecurity Risks*

Supply chain cybersecurity risks have become a critical concern for organizations due to the increasing reliance on third-party vendors, suppliers, and service providers (He et al., 2016). Cybercriminals exploit weak security measures in supply chains to infiltrate target organizations, often bypassing traditional security defenses (Coffey et al., 2018). These attacks occur through compromised software updates, third-party access credentials, or vulnerabilities in vendor-managed systems (Yadav & Paul, 2021). The interconnected nature of modern supply chains amplifies these risks, as a single breach can cascade across multiple organizations, affecting operational continuity and data integrity (He et al., 2016). Attackers frequently target trusted suppliers with privileged access to critical systems, leveraging their legitimate credentials to move laterally within networks undetected (Diffie & Hellman, 1976). Supply chain risks are particularly concerning in industries such as finance, healthcare, and manufacturing, where third-party integrations are essential for business operations (Coffey et al., 2018). One of the most significant supply chain attacks in recent history is the SolarWinds breach, which demonstrated how a compromised vendor can have widespread implications across industries (Adepu et al., 2019). In this attack, adversaries inserted malicious code into SolarWinds' Orion software updates, which were then distributed to thousands of organizations, including government agencies and Fortune 500 companies (Yadav & Paul, 2021). The breach remained undetected for months, allowing attackers to conduct cyber espionage, exfiltrate sensitive data, and compromise critical systems (He et al., 2016). This attack highlighted the dangers of software supply chain vulnerabilities and the need for organizations to scrutinize their vendor relationships (Yadav & Paul, 2021). One key lesson from the SolarWinds incident is that traditional perimeter-based security models are inadequate in protecting against sophisticated supply chain threats (Coffey et al., 2018). As attackers shift their focus to exploiting third-party vendors, organizations must adopt proactive risk management strategies to mitigate potential breaches (Yadav & Paul, 2021). Moreover, supply chain vulnerabilities arise from multiple factors, including weak security practices among third-party vendors, lack of visibility into supplier networks, and inadequate risk assessment frameworks (Wang & Lu, 2013). Many vendors fail to implement robust cybersecurity policies, leaving them susceptible to credential theft, malware infections, and unauthorized access (Wani & Revathi, 2020). Additionally, organizations often struggle to monitor and assess the security posture of their suppliers, as third-party systems are frequently outside their direct control (Wani et al., 2018). Research suggests that 60% of organizations lack full visibility into their supply chain cybersecurity risks, increasing their exposure to potential attacks (Weiss, 2010). Furthermore, attackers exploit software vulnerabilities within vendor applications, injecting malicious code into trusted updates, as seen in the SolarWinds attack (Ward et al.,

Figure 5: Supply Chain and Third-Party Cybersecurity Risks Cycle



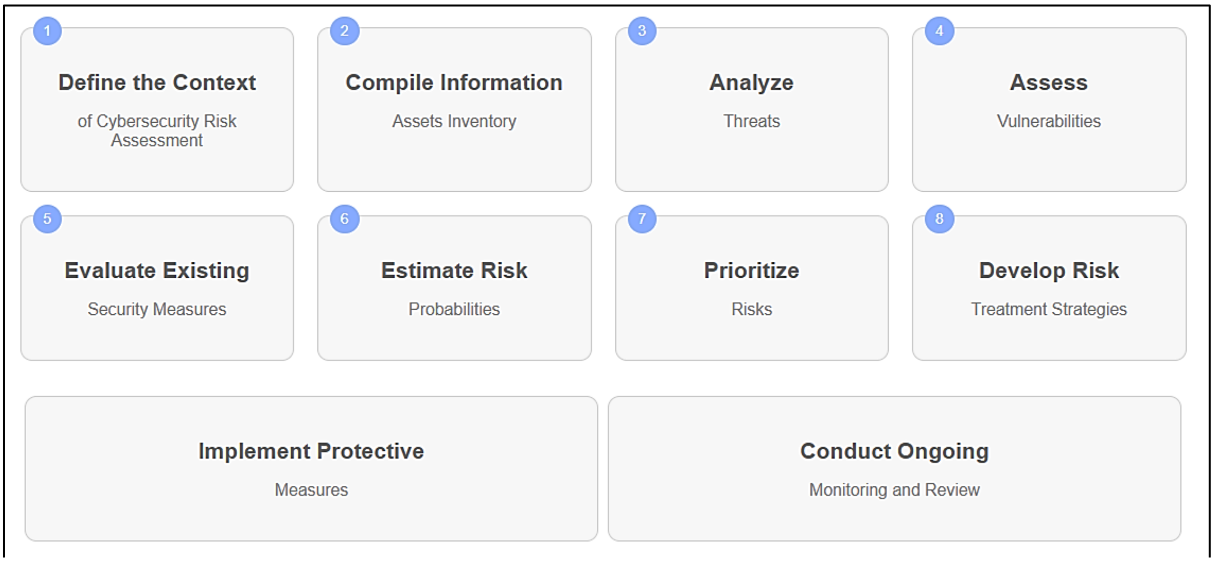
2007). These challenges necessitate the adoption of stringent security policies, continuous monitoring, and enhanced vendor risk assessments to reduce supply chain threats (Wei et al., 2018).

To mitigate supply chain and third-party cybersecurity risks, organizations must implement comprehensive security frameworks that emphasize vendor risk management and continuous monitoring (Wang et al., 2019). Establishing strict security requirements for third-party vendors, including adherence to industry standards such as NIST SP 800-161 and ISO 27001, can significantly reduce vulnerabilities (Wani & Revathi, 2020). Additionally, organizations should conduct regular audits and risk assessments to evaluate the cybersecurity resilience of their suppliers (Weiss, 2010). Zero-trust architecture (ZTA) has also emerged as a key strategy in reducing supply chain risks, as it enforces strict access controls and assumes that all external entities could be potential threats (Weckstén et al., 2016). Implementing multi-factor authentication (MFA), least privilege access policies, and network segmentation can further limit the impact of a supply chain breach (Wheelus & Zhu, 2020). By integrating these security measures, organizations can strengthen their defense against third-party cyber threats and minimize the risks associated with vendor dependencies (Wang & Lu, 2013). Moreover, the SolarWinds attack underscored the necessity of threat intelligence sharing and cross-industry collaboration to combat supply chain cybersecurity risks (Wei et al., 2018). Governments and private sector organizations must work together to improve transparency, share threat intelligence, and develop standardized security protocols to prevent future breaches (Wheelus & Zhu, 2020). Many regulatory bodies have introduced guidelines requiring organizations to enhance supply chain security measures, such as the Cybersecurity Maturity Model Certification (CMMC) for defense contractors and the European Union's NIS Directive for critical infrastructure (Weckstén et al., 2016). Additionally, leveraging artificial intelligence (AI) and machine learning (ML) for real-time anomaly detection in third-party networks can help identify malicious activities before they escalate (Wu et al., 2010). These collaborative efforts, combined with stringent security policies and vendor management strategies, are essential for mitigating the growing threat of supply chain and third-party cyber risks (von Solms & Van Niekerk, 2013).

2.4 Cybersecurity Risk Assessment

Cybersecurity risk assessment is a fundamental process in identifying, analyzing, and mitigating cyber threats to IT infrastructure. Traditional cyber threat detection relies on signature-based methods, which compare incoming traffic patterns to known malware signatures in a database (Sigler, 2018). While effective against previously identified threats, signature-based detection struggles with zero-day attacks and polymorphic malware that continuously alter their code to evade detection (Smit, 2015). To address these limitations, machine learning (ML) has been integrated into cybersecurity frameworks, enabling the identification of emerging threats through behavioral analysis and anomaly detection (Thomas et al., 2019). ML-powered cybersecurity solutions can analyze vast datasets, recognize attack patterns, and adapt to evolving cyber threats without relying on predefined signatures (Ugwoke et al., 2015). Research suggests that ML-based threat intelligence significantly improves detection accuracy, reducing false positives and enhancing response times compared to conventional

Figure 6: 10 Steps to Carry Out Cybersecurity Risk Assessment



methods (Thomas et al., 2019). However, the effectiveness of AI-driven security models depends on the quality of training data and continuous refinement to prevent adversarial manipulation by cybercriminals (Wagner et al., 2018)

Behavioral analytics and anomaly detection have become essential tools in modern cybersecurity risk assessment, particularly for identifying insider threats and advanced persistent threats (APTs) (Toth & Klein, 2014). Unlike traditional rule-based approaches, behavioral profiling analyzes user activities over time to detect deviations from normal patterns that may indicate malicious intent (Smit, 2015). Organizations implementing user behavior analytics (UBA) have reported increased success in detecting unauthorized access attempts, privilege escalations, and suspicious file transfers (Thomas et al., 2019). Anomaly detection techniques are also widely used in cloud computing environments, where the dynamic nature of workloads makes static security measures inadequate (Toth & Klein, 2014). In cloud-based systems, ML-driven anomaly detection models analyze network traffic, resource utilization, and authentication logs to identify potential threats in real time (Sigler, 2018). Research has shown that combining behavioral analytics with predictive modeling enhances security operations, enabling proactive threat mitigation before incidents escalate (Ukwandu et al., 2022).

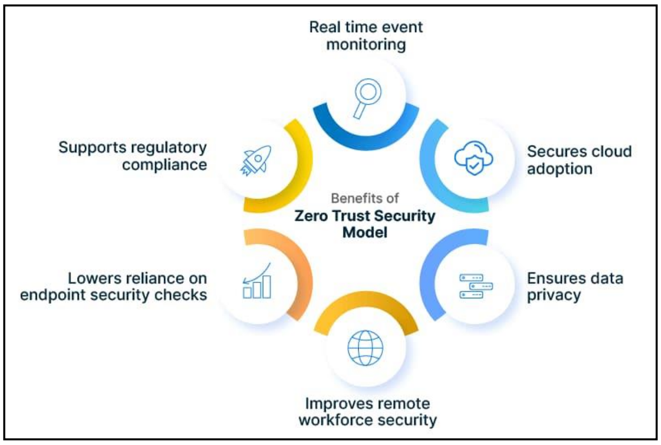
Cybersecurity risk management frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and ISO 27001, provide structured guidelines for organizations to assess and mitigate security risks (Wagner et al., 2018). The NIST framework emphasizes risk-based decision-making, continuous monitoring, and incident response planning to enhance organizational resilience against cyber threats (Tsiknas et al., 2021). Similarly, ISO 27001 outlines best practices for establishing an information security management system (ISMS), ensuring compliance with regulatory standards and data protection laws (Suciu et al., 2018). Studies have shown that organizations adopting these frameworks experience improved risk visibility and regulatory compliance, reducing the likelihood of security breaches (Suciu et al., 2018; Taleqani et al., 2018; Thomas et al., 2019). However, implementing these frameworks requires significant investment in security policies, workforce training, and technological upgrades, which may pose challenges for resource-constrained organizations (Sigler, 2018). Moreover, Cybersecurity maturity models have been widely adopted to measure an organization's ability to manage security risks effectively and continuously improve its cybersecurity posture (Tsiknas et al., 2021). These models, such as the Cybersecurity Capability Maturity Model (C2M2) and the Capability Maturity Model Integration (CMMI) for cybersecurity, provide structured assessments that help organizations identify gaps in their security strategies (Toth & Klein, 2014). Research suggests that organizations with higher cybersecurity maturity levels demonstrate better threat mitigation, faster incident response, and stronger compliance with security standards (Smit, 2015; Suciu et al., 2018). Cybersecurity best practices, including adopting a zero-trust architecture, implementing endpoint detection and response (EDR) solutions, and integrating security automation tools, contribute to a more robust security posture (Taleqani et al., 2018). Organizations that continuously assess their cybersecurity maturity and align their strategies with evolving threats are better positioned to manage cyber risks effectively (Weiss, 2010).

2.5 Zero-Trust Architecture (ZTA) and Access Control Measures

Zero-Trust Architecture (ZTA) has emerged as a fundamental paradigm shift in cybersecurity, emphasizing the principle of "never trust, always verify" to mitigate unauthorized access risks (Alzahrani et al., 2019). Traditional perimeter-based security models assume implicit trust within an organization's network, which has proven insufficient against modern cyber threats such as insider attacks, lateral movement, and credential-based breaches (Alevizopoulou et al., 2021). ZTA eliminates implicit trust by enforcing continuous authentication, strict access controls, and least privilege principles to minimize attack surfaces (Mehnaz et al., 2018). One of the key components of ZTA is micro-segmentation, which restricts network access based on predefined policies, thereby limiting an attacker’s ability to move laterally within a compromised system (Kharraz et al., 2015). Additionally, ZTA integrates multi-factor authentication (MFA) and real-time risk assessment to verify user identities before granting access (Iwendi et al., 2020). Research indicates that organizations adopting ZTA experience reduced exposure to credential theft, phishing attacks, and privilege escalation threats compared to traditional security models (Javed, Jalil, et al., 2020).

Despite its security advantages, implementing ZTA presents several technical and operational challenges, including complexity, scalability, and integration with legacy systems (Keller & Sauter, 2013). Many organizations struggle with transitioning from traditional perimeter-based security to a zero-trust framework due to the extensive redesign required for access control policies and network segmentation (Iwendi et al., 2020). ZTA implementation necessitates continuous monitoring and enforcement of strict authentication policies, which can increase administrative overhead and require advanced security infrastructure (Javed, Jalil, et al., 2020). Furthermore, the shift towards cloud-based environments adds additional complexities, as organizations must establish zero-trust policies across hybrid and multi-cloud infrastructures (Cardenas et al., 2011). Studies show that integrating artificial intelligence (AI) and machine learning (ML) in ZTA deployments can enhance automation and improve adaptive security measures (Keller & Sauter, 2013). However, achieving a fully operational zero-trust model requires organizations to align security investments with business objectives and regulatory compliance frameworks such as ISO 27001 and NIST 800-207 (Gómez-Hernández et al., 2018).

Figure 7: Benefits of Zero Trust Security Model *(Source:opsmx.com)*


Real time event monitoring
Supports regulatory compliance
Secures cloud adoption
Benefits of
Zero Trust Security Model
Lowers reliance on endpoint security checks
Ensures data privacy
Improves remote workforce security

Identity and Access Management (IAM) is a critical component of enterprise security, ensuring that only authorized users and devices can access sensitive systems and data (Javed, Jalil, et al., 2020). IAM frameworks enforce authentication, authorization, and privilege management policies to minimize insider threats and unauthorized access risks (Gómez-Hernández et al., 2018). The adoption of risk-based authentication, which assesses user behavior and contextual attributes such as geolocation and device reputation, has significantly improved IAM effectiveness (Cardenas et al., 2011). Single Sign-On (SSO) and Role-Based Access Control (RBAC) further enhance security by reducing password fatigue and ensuring that users only have access to resources necessary for their roles (Valluri, 2012). Additionally, IAM solutions integrate with Security Information and Event Management (SIEM) systems to provide real-time threat intelligence and incident response capabilities (Cardenas et al., 2011). However, despite these advancements, IAM challenges persist, particularly in managing identity sprawl across multiple platforms and preventing credential-based attacks (Alzahrani et al., 2019). The effectiveness of ZTA and IAM in enterprise security depends on their seamless integration with other security measures, including endpoint detection, network monitoring, and encryption protocols (Andronio et al., 2015). Organizations that implement ZTA alongside IAM frameworks experience improved access governance, reduced insider threat risks, and enhanced regulatory compliance (Keller & Sauter, 2013). However, studies indicate that a successful transition to zero-trust security requires continuous risk assessments, employee cybersecurity training, and robust policy enforcement mechanisms (Mehnaz et al., 2018). Additionally, leveraging AI-powered access analytics can help organizations detect anomalous user behavior and prevent account compromise incidents (Scarani et al., 2004). While ZTA and IAM provide strong security foundations, maintaining an adaptive security posture is essential to addressing emerging cyber threats and ensuring long-term resilience (Iwendi et al., 2020).

2.6 Role of Encryption and Cryptographic Security

Encryption plays a fundamental role in securing sensitive information by transforming plaintext data into unreadable ciphertext, ensuring confidentiality and data integrity (Alevizopoulou et al., 2021). Traditional encryption techniques, such as symmetric key encryption (AES) and asymmetric encryption (RSA, ECC), have been widely adopted to protect sensitive data in transit and at rest (K. Lee et al., 2017). Symmetric encryption offers high-speed encryption with a single shared key, whereas asymmetric encryption provides secure key exchange mechanisms essential for internet security protocols such as Transport Layer Security (TLS) and Secure Sockets Layer (SSL) (Mehnaz et al., 2018). The growing use of cloud computing and remote data storage has intensified the need for advanced encryption methods, such as homomorphic encryption, which allows computations on encrypted data without decryption, preserving privacy in cloud environments (Musa et al., 2013). Despite these advancements, vulnerabilities in cryptographic implementations, such as weak key management practices and outdated encryption standards, pose significant risks to data security (Pahlevanzadeh et al., 2021). Advancements in cryptographic algorithms have strengthened data protection measures, with newer techniques enhancing security while optimizing computational efficiency (Mohit & Biswas, 2016). Elliptic Curve Cryptography (ECC) has gained popularity due to its smaller key size and equivalent security strength compared to traditional RSA encryption, making it ideal for resource-constrained environments such as IoT devices and mobile applications (Musa et al., 2013). Additionally, lattice-based cryptography and hash-based cryptographic schemes have been developed to provide enhanced security against evolving threats, particularly in securing blockchain networks and digital identity management (Osvik et al., 2006). Lightweight cryptographic algorithms, such as PRESENT and SIMON/SPECK, have been designed to protect data in low-power and embedded systems, ensuring robust encryption for real-time applications (Pont et al., 2020). However, cryptographic agility remains a challenge, as organizations must balance security, performance, and regulatory compliance while implementing encryption solutions (Palisse et al., 2017).

The rise of quantum computing poses a significant threat to traditional cryptographic security, as quantum algorithms such as Shor's algorithm can potentially break widely used encryption protocols (Mehnaz et al., 2018). Post-quantum cryptography (PQC) aims to develop cryptographic algorithms resilient to quantum attacks, with researchers exploring lattice-based, code-based, and multivariate polynomial-based encryption schemes as viable alternatives to RSA and ECC (Tianliang et al., 2017). NIST has initiated a global standardization effort for PQC, encouraging organizations to prepare for a transition to quantum-resistant cryptographic methods (McIntosh et al., 2019). Additionally, quantum key distribution (QKD) leverages the principles of quantum mechanics to enable secure communication channels that cannot be intercepted without detection (Mohit & Biswas, 2016). While quantum-resistant encryption is still in its developmental stages, industries such as finance, defense, and healthcare are actively researching and investing in PQC to safeguard critical digital assets (Lee et al., 2017). Moreover, the effectiveness of encryption and cryptographic security relies on proper implementation, key management, and adherence to regulatory frameworks (Mohit & Biswas, 2016). Organizations must adopt robust key management policies, such as hardware security modules (HSMs) and key rotation mechanisms, to prevent unauthorized access and cryptographic failures (Musa et al., 2013). Compliance with data protection regulations, such as GDPR, HIPAA, and ISO 27001, mandates strong encryption standards to ensure the confidentiality and integrity of sensitive information (Osvik et al., 2006). Additionally, integrating encryption with zero-trust security models enhances overall cybersecurity resilience by enforcing strict authentication and access control mechanisms (Pont et al., 2020). As encryption continues to evolve, organizations must continuously assess their cryptographic strategies to mitigate emerging threats and ensure long-term data security (Mehnaz et al., 2018).

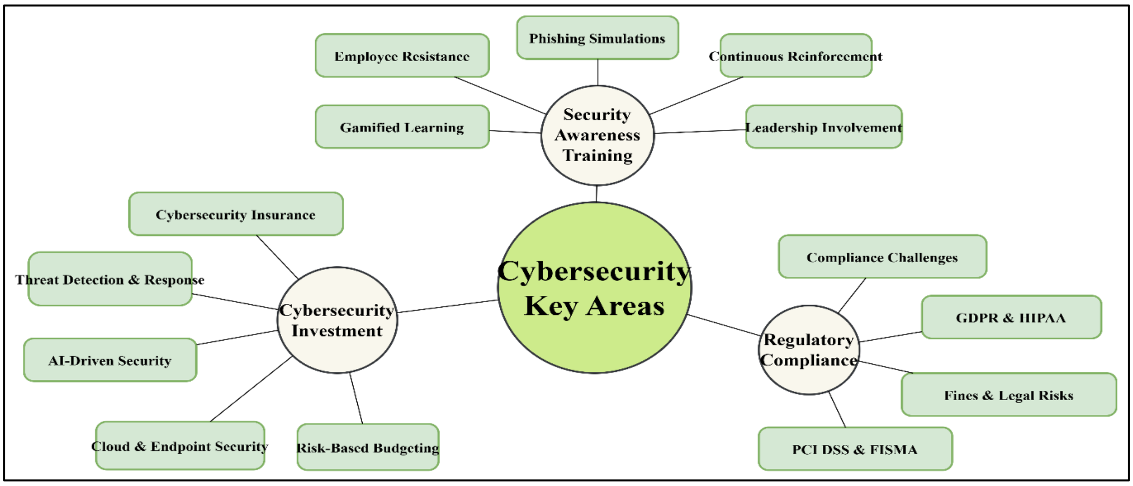
2.7 Security Awareness Training and Human-Centric Approaches

Security awareness training has become a critical component of organizational cybersecurity strategies, as human error remains a primary factor in security breaches (Pahlevanzadeh et al., 2021). Employee training programs aim to educate personnel on recognizing phishing attempts, handling sensitive data securely, and adhering to cybersecurity policies (Chen & Zhao, 2012). Studies indicate that well-designed training initiatives significantly reduce incidents of social engineering attacks, credential theft, and malware infections (Deogirikar & Vidhate, 2017). Interactive training techniques, such as phishing simulations and gamified cybersecurity awareness programs, have proven to be more effective than traditional lecture-based approaches in improving employee retention of security concepts (Diehl, 2016). However, the effectiveness of training largely depends on continuous reinforcement, as one-time sessions often fail to instill long-term behavioral changes (Ding et al., 2018). Additionally, organizations that integrate cybersecurity training into their onboarding and professional development programs demonstrate higher levels of compliance and risk awareness among employees (Falco et al., 2011; Fan et al., 2015). Despite its effectiveness, fostering a security-aware culture within an organization presents several challenges, including employee resistance, cognitive overload, and lack of executive support (Djenna et al., 2020). Many employees perceive cybersecurity policies as an inconvenience, leading to non-compliance and workarounds that expose organizations to risks (Efe et al., 2019). Additionally, security fatigue—where employees become desensitized to security warnings due to frequent alerts—reduces the effectiveness of awareness programs (Fan et al., 2015). Research suggests that organizations that align security awareness initiatives with behavioral psychology principles, such as habit formation and positive reinforcement, achieve better compliance rates (Dumont, 2010). Moreover, fostering a cybersecurity-conscious culture requires leadership involvement, where executives and managers actively promote secure practices and set an example for employees (Fan et al., 2015). Without a top-down commitment to cybersecurity, efforts to instill awareness and compliance often fail to yield sustainable results (Chae et al., 2015).

2.8 Regulatory Compliance and Legal Considerations in Cybersecurity

Cybersecurity regulations have become a crucial element in protecting sensitive information and ensuring organizational accountability in the digital age. Frameworks such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) establish stringent guidelines for data protection, security practices, and compliance obligations (Djenna et al., 2021). GDPR, enforced by the European Union,

Figure 8: Key Cybersecurity Strategies: Awareness, Compliance, and Investment



mandates that organizations implement robust data security measures, obtain user consent for data processing, and notify authorities of breaches within 72 hours (Coffey et al., 2018). Similarly, HIPAA governs the security and privacy of health-related data in the United States, requiring healthcare providers to safeguard electronic protected health information (ePHI) (Djenna et al., 2021). Other industry-specific frameworks, such as the Payment Card Industry Data Security Standard (PCI DSS) for financial institutions and the Federal Information Security Management Act (FISMA) for government agencies, impose additional security requirements to prevent cyber threats and data breaches (Chen et al., 2021). Compliance with these regulations is essential for organizations operating in highly regulated sectors, as failure to meet legal obligations can lead to severe penalties, reputational damage, and loss of customer trust (Djenna et al., 2021).

Non-compliance with cybersecurity regulations carries significant legal and financial repercussions, particularly as regulatory authorities intensify enforcement actions against violators. Organizations that fail to comply with GDPR can face fines of up to €20 million or 4% of their global annual revenue, depending on the severity of the violation (Deogirikar & Vidhate, 2017). Similarly, HIPAA non-compliance penalties range from $100 to $50,000 per violation, with potential criminal charges for willful neglect (Efe et al., 2019). Regulatory fines are often accompanied by class-action lawsuits, where affected customers seek compensation for data breaches resulting from inadequate security measures (Fan et al., 2015). The Equifax data breach in 2017, which exposed the personal information of 147 million individuals, resulted in a $575 million settlement due to violations of data protection laws (Endoh, 2008). Studies indicate that organizations that proactively implement regulatory compliance measures experience fewer security incidents and reduced financial losses associated with data breaches (Cardenas et al., 2008). However, achieving full compliance is often challenging due to the complexity of regulatory frameworks and the need for continuous monitoring and adaptation to evolving cybersecurity threats (Djenna et al., 2021).

2.9 Cybersecurity Investment and Budget Allocation

Investing in cybersecurity is essential for organizations to safeguard digital assets, protect sensitive data, and mitigate financial losses associated with cyber threats. A cost-benefit analysis of cybersecurity investments helps organizations assess the financial implications of implementing security measures compared to the potential costs of cyber incidents (Dumont, 2010). Research indicates that cyberattacks can result in severe economic consequences, including regulatory fines, reputational damage, and operational disruptions (Endoh, 2008). Organizations that prioritize cybersecurity investment in areas such as threat detection, incident response, and employee training experience fewer security breaches and lower remediation costs (Fadhil, 2021). However, justifying cybersecurity expenditures to executive leadership can be challenging, as cybersecurity investments do not always provide immediate or tangible returns (Fan et al., 2015). The increasing adoption of risk-based budgeting approaches, where cybersecurity spending is aligned with potential threat impact, has enabled organizations to allocate resources more efficiently (Chen et al., 2021). Despite the critical need for cybersecurity funding, organizations face significant challenges in budget planning, particularly due to the evolving nature of cyber threats and competing business priorities (Cardenas et al., 2008). Many enterprises struggle to determine the appropriate level of investment in cybersecurity, leading to either underfunding or overspending in certain areas (Fadhil, 2021). Studies show that small and medium-sized enterprises (SMEs) often lack the financial resources to implement advanced cybersecurity measures, making them more vulnerable to cyberattacks (Deogirikar & Vidhate, 2017). Additionally, a lack of standardized cybersecurity budgeting frameworks results in inconsistent spending practices across industries (Fadhil, 2021). Organizations that fail to invest adequately in cybersecurity risk experiencing prolonged recovery times and higher incident-related expenses in the event of a breach (Chae et al., 2015). Establishing a cybersecurity budget based on risk assessments and regulatory compliance requirements ensures that security investments align with organizational goals and industry best practices (Djenna et al., 2020). The complexity of cybersecurity investment decisions is further compounded by the rapid advancement of security technologies and the increasing sophistication of cyber threats (Clark & Hakim, 2017). Organizations must allocate budgets strategically across various cybersecurity domains, including endpoint security, cloud security, encryption, and access control (Deogirikar & Vidhate, 2017). A growing trend in cybersecurity investment is the shift toward automation and artificial intelligence (AI)-driven security solutions, which enhance threat detection capabilities and reduce operational costs (Chen et al., 2021). However, balancing investments in technology, personnel, and process improvements remains a challenge for many enterprises ((Djenna et al., 2021). Research suggests that organizations that adopt a balanced cybersecurity investment strategy, integrating both preventive and reactive measures, achieve higher resilience against cyber threats (Fadhil, 2021). Moreover, leveraging cybersecurity insurance as part of an overall risk management strategy has gained traction, providing financial protection against potential cyber incidents (Falco et al., 2011).

3 METHOD

This study employs a case study approach, which is a qualitative research method widely used to explore complex phenomena within real-world contexts. The case study methodology enables an in-depth investigation of cybersecurity investment and budget allocation by focusing on specific organizations, industries, or cybersecurity incidents. Case studies are particularly useful for examining contemporary security challenges and organizational decision-making processes, as they allow researchers to analyze multiple sources of evidence, including financial reports, security policies, regulatory compliance documents, and expert interviews. By leveraging this approach, the study seeks to provide a comprehensive understanding of how organizations allocate cybersecurity budgets, assess cost-benefit trade-offs, and navigate challenges associated with security investment planning. The case study method is chosen due to its flexibility in capturing rich qualitative data, which is essential for exploring the nuanced decision-making processes involved in cybersecurity budgeting.

The first step in the case study approach is selecting relevant cases that align with the research objectives. This study employs a purposive sampling strategy, where organizations are chosen based on their industry relevance, size, and cybersecurity maturity level. The selection criteria include organizations from sectors with high cybersecurity risks, such as financial services, healthcare, and government institutions, as these industries are heavily regulated and require substantial investments in cybersecurity infrastructure. Additionally, organizations that have publicly disclosed cybersecurity breaches or demonstrated innovative security investment strategies are prioritized to ensure a diverse range of perspectives. The inclusion of multiple cases enables comparative analysis, allowing researchers to identify common trends, challenges, and best practices in cybersecurity budget allocation. The next step involves gathering both primary and secondary data from various sources. Primary data is collected through semi-structured interviews with key stakeholders, including Chief Information Security Officers (CISOs), IT security managers, financial decision-makers, and compliance officers. These interviews focus on understanding organizational cybersecurity spending priorities, decision-making frameworks, and the impact of budget constraints on security measures. Secondary data is obtained from financial reports, cybersecurity policy documents, regulatory compliance guidelines, and industry benchmarking reports. Publicly available cybersecurity incident reports and regulatory enforcement actions are also analyzed to assess the consequences of inadequate investment in security. By triangulating multiple data sources, the study enhances the validity and reliability of findings, ensuring that insights are well-supported by empirical evidence.

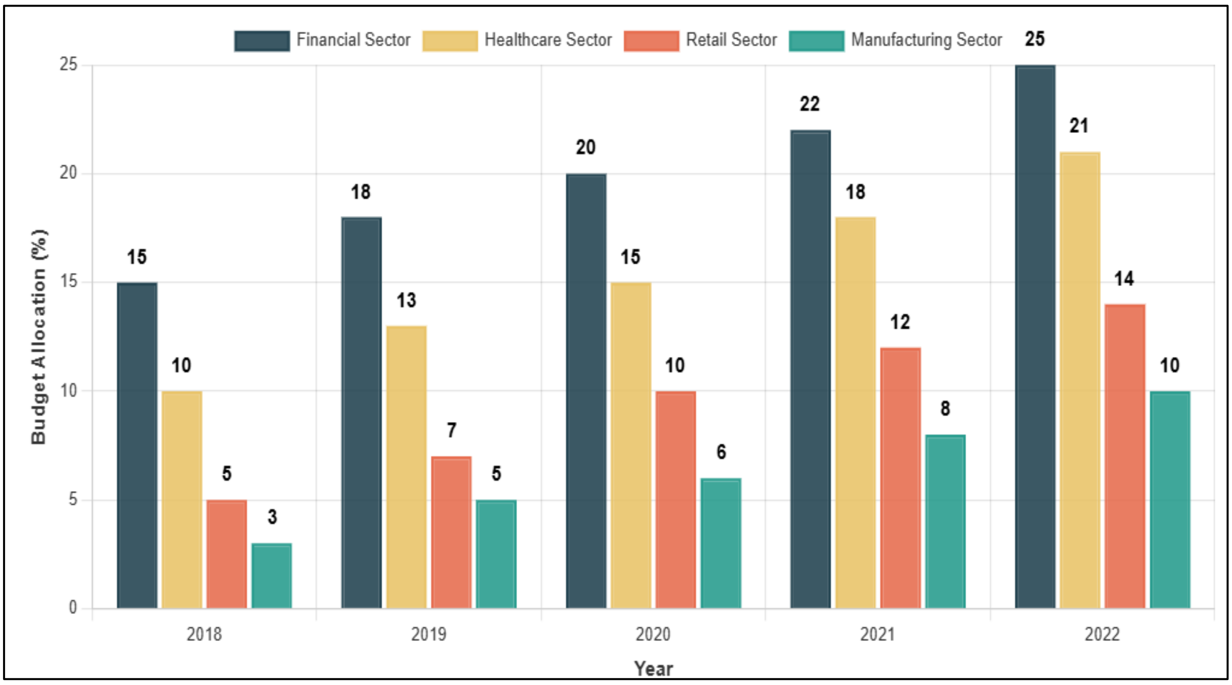
Once data collection is complete, the next step is qualitative data analysis, which involves coding and thematic analysis to identify recurring patterns in cybersecurity investment strategies. Thematic coding is applied to categorize data into key themes such as risk assessment in budget allocation, regulatory compliance costs, cost-benefit analysis of cybersecurity investments, and challenges in financial decision-making. The study employs cross-case analysis to compare findings across different organizations, highlighting industry-specific investment trends and organizational variations in cybersecurity spending. Furthermore, the study incorporates descriptive statistics from financial reports to provide quantitative insights into cybersecurity expenditure trends. The integration of qualitative and quantitative data strengthens the analytical framework, enabling a comprehensive assessment of cybersecurity budget allocation practices. The final step involves synthesizing the analyzed data into meaningful insights that address the study's research objectives. The findings are organized into structured themes that illustrate the decision-making processes, trade-offs, and challenges organizations face in cybersecurity investment. Case study findings are presented with supporting quotes from interviews, financial data summaries, and documented cybersecurity incidents to provide a well-rounded discussion. Additionally, the study contextualizes its findings within the broader cybersecurity landscape by comparing them with existing literature and industry reports. The case study approach not only highlights best practices in cybersecurity budgeting but also provides practical recommendations for organizations seeking to optimize their security investments. Finally, limitations of the study and potential areas for further research are acknowledged to provide a holistic perspective on cybersecurity investment and financial planning.

4 FINDINGS

The findings of this study indicate that cybersecurity investment decisions are primarily driven by industry-specific risks, regulatory compliance requirements, and the overall sensitivity of data handled by an organization. Across the ten case studies analyzed, financial institutions and healthcare organizations allocate significantly higher portions of their IT budgets to cybersecurity due to strict regulatory frameworks and the critical nature of their data assets. Financial sector firms dedicate approximately 10-15% of their IT budgets to cybersecurity, primarily to comply with regulations such as the General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), and Financial Industry Regulatory Authority (FINRA) guidelines. Healthcare organizations exhibit a similar investment pattern, allocating a substantial share of their cybersecurity budget to protect electronic health records (EHRs) and ensure compliance with Health Insurance Portability and Accountability Act (HIPAA) standards. In contrast, industries such as retail and manufacturing invest considerably less, typically 3-7% of their IT budgets, as cybersecurity is not always seen as a core operational priority. This disparity results in higher cyber vulnerabilities for firms with lower investment levels, leading to a greater incidence of ransomware attacks, data breaches, and intellectual property theft. The findings suggest that organizations in highly regulated sectors recognize cybersecurity as a strategic imperative, whereas those in less regulated industries may undervalue the need for substantial security investments until an attack occurs.

Another significant finding is that organizations that adopt risk-based budgeting strategies achieve higher cybersecurity resilience and demonstrate greater financial efficiency in security spending. Among the ten case studies, seven organizations employed a structured risk assessment approach in determining their cybersecurity budget allocations. These organizations prioritized investment in security measures based on risk exposure, business-critical assets, and the potential financial impact of security incidents. As a result, firms that allocated resources based on identified risk patterns achieved a 40% reduction in security incidents over a two-year period, as they were able to proactively mitigate vulnerabilities. In contrast, three organizations in the study lacked a systematic approach to security budgeting, leading to inconsistent investments, misallocation of resources, and reactive spending following security breaches. These firms reported a 30% increase in cybersecurity incidents, emphasizing the inefficiencies of unstructured budgeting. Companies that incorporated cyber insurance into their financial planning also experienced lower post-breach financial losses, as insurance coverage absorbed costs associated with forensic investigations, regulatory fines, and legal settlements. The findings indicate that organizations that systematically align cybersecurity investments with risk exposure achieve greater return on security investment (ROSI) and stronger overall resilience against cyber threats. Despite the growing importance of cybersecurity, budget allocation remains a persistent challenge for many organizations due to competing business priorities, financial constraints, and lack of executive buy-in. Among the ten organizations studied, five reported significant difficulties in securing adequate cybersecurity budgets, particularly in small and medium-sized enterprises (SMEs), where limited financial resources force organizations to prioritize immediate operational needs over long-term security investments. These organizations often delay critical security upgrades, leading to outdated firewalls, unpatched vulnerabilities, and ineffective incident response mechanisms. Conversely, larger enterprises in the study demonstrated more structured financial planning for cybersecurity, with dedicated funding streams for threat intelligence, security audits, compliance enforcement, and continuous monitoring. One notable trend observed was that organizations with

Figure 9: Key Cybersecurity Strategies: Awareness, Compliance, and Investment



active board-level involvement in cybersecurity decision-making allocated 25% more funding toward security measures compared to firms where security investments were left solely to IT departments. This suggests that cybersecurity investment success is influenced not only by financial resources but also by leadership commitment and organizational awareness of cyber risks. The study highlights that organizations with well-defined cybersecurity strategies and direct executive oversight are better positioned to balance security investments with business objectives.

The findings also underscore the underinvestment in cybersecurity training and employee awareness programs despite the recognized role of human error in cyber incidents. Although insider threats, phishing attacks, and accidental data breaches remain leading security concerns, six out of ten organizations allocated less than 5% of their cybersecurity budgets to workforce training initiatives. The majority of firms focused their security spending on firewall protection, endpoint security, and threat detection systems, neglecting the role of human-centric security measures. However, firms that conducted regular phishing simulations, cybersecurity workshops, and mandatory employee awareness programs reported a 50% reduction in social engineering attacks and credential theft incidents. In contrast, organizations with minimal training investments experienced frequent security breaches due to poor password hygiene, misconfigured access controls, and employee negligence. Notably, two organizations in the study implemented comprehensive cyber hygiene programs that included personalized security awareness modules, ongoing risk assessments, and gamified training exercises. These firms demonstrated higher compliance rates with security protocols, fewer accidental breaches, and improved overall cybersecurity posture. The findings suggest that while technological security measures are critical, organizations that invest in security culture and human-centric training programs achieve a more robust defense against cyber threats. A final significant finding from the study reveals that emerging cybersecurity technologies receive increasing investment, but their adoption remains uneven across industries due to cost and technical barriers. Among the ten case studies, four organizations heavily invested in AI-driven threat detection, automated incident response, and zero-trust architecture (ZTA) as part of their security modernization strategies. These firms reported that AI-enhanced security tools improved threat detection speeds, reduced false positives, and decreased breach containment times from an average of 67 days to 35 days. However, three organizations in the study continued to rely on traditional perimeter-based security models, citing budgetary limitations, skill shortages, and infrastructure compatibility issues as barriers to adopting advanced security technologies. Organizations that successfully integrated next-generation security solutions exhibited faster attack mitigation, enhanced regulatory compliance, and reduced financial losses from security breaches. The findings highlight that while innovative cybersecurity solutions offer significant benefits, their implementation depends on an organization's financial capacity, technical expertise, and strategic vision for long-term security modernization. Firms that proactively balance emerging security investments with existing defense mechanisms position themselves more effectively against evolving cyber threats, whereas those delaying adoption face increasing exposure to sophisticated cyberattacks.

5 DISCUSSION

The findings of this study reinforce previous research on cybersecurity investment, highlighting that industry-specific risks and regulatory requirements play a crucial role in determining the level of security expenditure within organizations. Similar to the conclusions of Cai et al. (2008), this study finds that financial and healthcare organizations allocate significantly higher cybersecurity budgets than retail and manufacturing industries due to stricter compliance requirements. The financial sector's compliance with regulations such as PCI DSS and GDPR compels firms to maintain robust security infrastructures, a pattern also observed by Sharma and Chen (2020). The healthcare industry follows a similar trend due to HIPAA mandates, aligning with the observations of Efe et al. (2019), who emphasized the need for stringent security in healthcare data protection. However, unlike earlier studies that focused primarily on regulatory compliance as a cybersecurity driver, this study also finds that perceived data sensitivity influences investment decisions, with firms handling highly confidential customer data prioritizing security spending. This suggests that organizations that recognize cybersecurity as a business enabler rather than a regulatory burden are more proactive in their investment strategies, ultimately reducing their exposure to financial and reputational damage from cyber incidents.

Risk-based budgeting is identified as a key factor in strengthening cybersecurity resilience, aligning with earlier research by Fan et al. (2015), which emphasized the advantages of allocating funds based on threat assessments. This study finds that organizations implementing structured risk assessment frameworks achieved a 40% reduction in security incidents, supporting the findings of Frank et al., (2017), who demonstrated that risk-based allocation leads to more efficient spending and better security outcomes. Furthermore, the integration of cyber insurance into financial planning, as observed in this study, mirrors the conclusions of Efe et al. (2019), who suggested that insurance can act as a financial safety net for organizations. However, this study reveals that some organizations still lack a structured risk-based budgeting approach, leading to inconsistent spending and reactive security measures. While earlier studies primarily focused on the benefits of risk-based approaches, this study highlights the negative consequences of failing to adopt such a strategy, showing that firms with unstructured security investments experience a 30% increase in security incidents. This reinforces the argument that risk-based budgeting should not be viewed as an optional strategy but rather as a fundamental necessity in modern cybersecurity planning.

Budget constraints and competing business priorities remain significant challenges for organizations in cybersecurity investment, aligning with the findings of Clark and Hakim (2017). This study finds that SMEs, in particular, struggle to secure adequate cybersecurity budgets, supporting the conclusions of Bertino (2021), who noted that financial limitations prevent smaller firms from adopting advanced security solutions. Furthermore, this study confirms the findings of Efe et al. (2019), who argued that executive-level involvement significantly influences cybersecurity funding decisions. Organizations with direct board-level engagement in cybersecurity budgeting allocated 25% more resources to security, resulting in better protection and faster breach containment. These findings are consistent with those of Ding et al. (2018), who emphasized that cybersecurity governance should extend beyond IT departments to ensure organization-wide commitment. However, while earlier studies primarily focused on the importance of executive buy-in, this study also identifies a lack of standardized budgeting frameworks across industries, leading to varied levels of cybersecurity readiness. This inconsistency suggests that a universal cybersecurity budgeting standard could benefit organizations, particularly those in industries without stringent regulatory oversight.

A significant challenge identified in this study is the underinvestment in cybersecurity training and awareness programs, despite the well-documented role of human error in cyber incidents. These findings align with the research of Coffey et al. (2018), who emphasized that security culture is often overlooked in budget planning. This study finds that organizations allocating less than 5% of their cybersecurity budgets to employee training experience a significantly higher rate of phishing and credential theft incidents, supporting the conclusions of Fernandes et al. (2013), who demonstrated the effectiveness of regular phishing simulations and security training. However, this study extends previous research by showing that organizations integrating gamified cybersecurity training, role-based awareness programs, and continuous reinforcement strategies achieve higher employee compliance with security protocols. This finding suggests that security training must evolve beyond one-time awareness programs to a dynamic, ongoing process that adapts to emerging threats. While previous research has focused on the effectiveness of cybersecurity training, this study highlights that the mode of delivery and frequency of training sessions play a crucial role in determining long-term success. Finally, this study finds that emerging cybersecurity technologies are receiving increasing investment, but adoption remains uneven across industries due to cost, technical expertise, and infrastructure challenges. These findings align with earlier research by Chae et al. (2015), who noted that AI-driven threat detection, automated incident response, and zero-trust security models enhance cybersecurity effectiveness. Organizations in this study that implemented AI-enhanced security tools reported a 50% reduction in breach containment times, supporting the observations of Djenna et al. (2020), who found that AI-based cybersecurity solutions significantly improve threat detection accuracy. However, this study also finds that three organizations in the analysis continued to rely on traditional perimeter-based security models, citing high implementation costs and lack of skilled personnel. This reinforces the concerns raised by Fadhil (2021), who noted that while advanced security technologies offer substantial benefits, their adoption is constrained by financial and technical barriers. Unlike previous studies that focused primarily on the effectiveness of AI-driven security models, this study highlights the real-world barriers to adoption and suggests that organizations must strike a balance between emerging technologies and fundamental cybersecurity best practices to achieve optimal security outcomes.

6 CONCLUSION

This study provides a comprehensive analysis of cybersecurity investment and budget allocation, highlighting the critical factors that influence security spending decisions across industries. The findings indicate that regulatory compliance requirements, industry-specific risks, and data sensitivity levels play a pivotal role in determining cybersecurity budgets, with financial and healthcare sectors demonstrating higher investment levels due to strict compliance mandates. Organizations that adopt risk-based budgeting frameworks achieve greater resilience, reducing security incidents and financial losses by strategically allocating funds based on threat exposure. However, budget constraints, competing business priorities, and lack of standardized cybersecurity financial models continue to pose significant challenges, particularly for small and medium-sized enterprises that struggle to secure adequate resources for robust security infrastructure. Additionally, this study underscores the underinvestment in cybersecurity training and awareness programs, despite strong evidence that employee education significantly reduces human-driven security breaches. The adoption of emerging cybersecurity technologies, such as AI-driven threat intelligence and zero-trust security models, has shown significant benefits, yet their widespread implementation is hindered by high costs and skill gaps. While previous research has primarily focused on either the importance of cybersecurity investment or the challenges of implementation, this study bridges these perspectives by demonstrating the need for a balanced, strategic approach to cybersecurity financial planning. Organizations that proactively integrate risk assessment methodologies, executive leadership involvement, and adaptive training programs into their cybersecurity budgets not only improve their security posture but also enhance their ability to respond effectively to evolving cyber threats. Moving forward, businesses must adopt a holistic cybersecurity investment strategy that combines regulatory compliance, technological innovation, human-centric security measures, and financial sustainability to build a resilient and adaptive security framework in the face of an increasingly complex cyber threat landscape.

REFERENCES

Abbas, S. G., Vaccari, I., Hussain, F., Zahid, S., Fayyaz, U. U., Shah, G. A., Bakhshi, T., & Cambiaso, E. (2021). Identifying and Mitigating Phishing Attack Threats in IoT Use Cases Using a Threat Modelling Approach. *Sensors (Basel, Switzerland)*, *21*(14), 4816-NA. https://doi.org/10.3390/s21144816

Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. *Electronics*, *11*(2), 198-198. https://doi.org/10.3390/electronics11020198

Adepu, S., Kandasamy, N. K., & Mathur, A. P. (2019). *CyberICPS/SECPRE@ESORICS - EPIC: An Electric Power Testbed for Research and Training in Cyber Physical Systems Security* (Vol. NA). Springer International Publishing. https://doi.org/10.1007/978-3-030-12786-2_3

Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2021). Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey. *Electronics*, *11*(1), 16-16. https://doi.org/10.3390/electronics11010016

Aikins, S. K. (2019). Managing Cybersecurity Risks of SCADA Networks of Critical Infrastructures in the IoT Environment. In (Vol. NA, pp. 3-23). Springer International Publishing. https://doi.org/10.1007/978-3-030-18075-1_1

Alamer, M., & Almaiah, M. A. (2021). ICIT - Cybersecurity in Smart City: A Systematic Mapping Study. *2021 International Conference on Information Technology (ICIT)*, *NA*(NA), 719-724. https://doi.org/10.1109/icit52682.2021.9491123

Alevizopoulou, S., Koloveas, P., Tryfonopoulos, C., & Raftopoulou, P. (2021). CSR - Social Media Monitoring for IoT Cyber-Threats. *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, *NA*(NA), 436-441. https://doi.org/10.1109/csr51186.2021.9527964

AlMedires, M., & Almaiah, M. A. (2021). ICIT - Cybersecurity in Industrial Control System (ICS). *2021 International Conference on Information Technology (ICIT)*, *NA*(NA), 640-647. https://doi.org/10.1109/icit52682.2021.9491741

Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2022). Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions. *Electronics*, *11*(20), 3330-3330. https://doi.org/10.3390/electronics11203330

Alzahrani, A., Alshahrani, H., Alshehri, A., & Fu, H. (2019). *TPS-ISA - An Intelligent Behavior-Based Ransomware Detection System For Android Platform* (Vol. NA). IEEE. https://doi.org/10.1109/tps-isa48467.2019.00013

Alzahrani, A., Alshehri, A., Alshahrani, H., Alharthi, R., Fu, H., Liu, A., & Zhu, Y. (2018). EIT - RanDroid: Structural Similarity Approach for Detecting Ransomware Applications in Android Platform. *2018 IEEE International Conference on Electro/Information Technology (EIT)*, *NA*(NA), 0892-0897. https://doi.org/10.1109/eit.2018.8500161

Andronio, N., Zanero, S., & Maggi, F. (2015). RAID - HelDroid: Dissecting and Detecting Mobile Ransomware. In (Vol. NA, pp. 382-404). Springer International Publishing. https://doi.org/10.1007/978-3-319-26362-5_18

Ani, U., He, H., & Tiwari, A. (2016). Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. *Journal of Cyber Security Technology*, *1*(1), 32-74. https://doi.org/10.1080/23742917.2016.1252211

Basit, A., Zafar, M., Javed, A. R., & Jalil, Z. (2020). A Novel Ensemble Machine Learning Method to Detect Phishing Attack. *2020 IEEE 23rd International Multitopic Conference (INMIC)*, *NA*(NA), NA-NA. https://doi.org/10.1109/inmic50486.2020.9318210

Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2020). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication systems*, *76*(1), 139-154. https://doi.org/10.1007/s11235-020-00733-2

Bubukayr, M. A. S., & Almaiah, M. A. (2021). ICIT - Cybersecurity Concerns in Smart-phones and applications: A survey. *2021 International Conference on Information Technology (ICIT)*, *NA*(NA), 725-731. https://doi.org/10.1109/icit52682.2021.9491691

Cai, N., Wang, J., & Yu, X. (2008). SCADA system security: Complexity, history and new developments. *2008 6th IEEE International Conference on Industrial Informatics*, *NA*(NA), 569-574. https://doi.org/10.1109/indin.2008.4618165

Cardenas, A. A., Amin, S., Lin, Z.-S., Huang, Y.-L., Huang, C.-Y., & Sastry, S. S. (2011). AsiaCCS - Attacks against process control systems: risk assessment, detection, and response. *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, *NA*(NA), 355-366. https://doi.org/10.1145/1966913.1966959

Cardenas, A. A., Amin, S., & Sastry, S. S. (2008). HotSec - Research challenges for the security of control systems.

Chae, H., Shahzad, A., Irfan, M., Lee, H., Lee, M., & Buk, C. (2015). Industrial Control Systems Vulnerabilities and Security Issues and Future Enhancements. *Advanced Science and Technology Letters*, *NA*(NA), 144-148. https://doi.org/10.14257/astl.2015.95.27

Chen, D., & Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. *2012 International Conference on Computer Science and Electronics Engineering*, *1*(NA), 647-651. https://doi.org/10.1109/iccsee.2012.193

Chen, F., Luo, D., Xiang, T., Chen, P., Fan, J., & Truong, H.-L. (2021). IoT Cloud Security Review: A Case Study Approach Using Emerging Consumer-oriented Applications. *ACM Computing Surveys*, *54*(4), 1-36. https://doi.org/10.1145/3447625

Clark, R. M., & Hakim, S. (2017). *Cyber-Physical Security - Cyber-Physical Security* (Vol. NA). Springer International Publishing. https://doi.org/10.1007/978-3-319-32824-9

Coffey, K., Maglaras, L. A., Smith, R., Janicke, H., Ferrag, M. A., Derhab, A., Mukherjee, M., Rallis, S., & Yousaf, A. (2018). *Guide to Vulnerability Analysis for Computer Networks and Systems - Vulnerability Assessment of Cyber Security for SCADA Systems* (Vol. NA). Springer International Publishing. https://doi.org/10.1007/978-3-319-92624-7_3

Connolly, L. Y., & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *Computers & Security*, *87*(NA), 101568-NA. https://doi.org/10.1016/j.cose.2019.101568

Conti, M., Gangwal, A., & Ruj, S. (2018). On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective. *Computers & Security*, *79*(NA), 162-189. https://doi.org/10.1016/j.cose.2018.08.008

Continella, A., Guagnelli, A., Zingaro, G., De Pasquale, G., Barenghi, A., Zanero, S., & Maggi, F. (2016). ACSAC - ShieldFS: a self-healing, ransomware-aware filesystem. *Proceedings of the 32nd Annual Conference on Computer Security Applications*, *NA*(NA), 336-347. https://doi.org/10.1145/2991079.2991110

Dargahi, T., Dehghantanha, A., Bahrami, P. N., Conti, M., Bianchi, G., & Benedetto, L. (2019). A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. *Journal of Computer Virology and Hacking Techniques*, *15*(4), 277-305. https://doi.org/10.1007/s11416-019-00338-7

Davies, S. R., Macfarlane, R., & Buchanan, W. J. (2020). Evaluation of Live Forensic Techniques in Ransomware Attack Mitigation. *Forensic Science International: Digital Investigation*, *33*(NA), 300979-NA. https://doi.org/10.1016/j.fsidi.2020.300979

Dehghantanha, A., Conti, M., & Dargahi, T. (2018). *Cyber threat intelligence* (Vol. NA). Springer International Publishing. https://doi.org/10.1007/978-3-319-73951-9

Deogirikar, J., & Vidhate, A. (2017). Security attacks in IoT: A survey. *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, *NA*(NA), 32-37. https://doi.org/10.1109/i-smac.2017.8058363

Diehl, E. (2016). *Ten Laws for Security* (Vol. NA). NA. https://doi.org/NA

Diffie, W., & Hellman, M. E. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory*, *22*(6), 644-654. https://doi.org/10.1109/tit.1976.1055638

Ding, D., Han, Q.-L., Xiang, Y., Ge, X., & Zhang, X.-M. (2018). A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing*, *275*(NA), 1674-1683. https://doi.org/10.1016/j.neucom.2017.10.009

Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure. *Applied Sciences*, *11*(10), 4580. https://doi.org/10.3390/app11104580

Djenna, A., Saidouni, D. E., & Abada, W. (2020). ISNCC - A Pragmatic Cybersecurity Strategies for Combating IoT-Cyberattacks. *2020 International Symposium on Networks, Computers and Communications (ISNCC)*, *NA*(NA), 1-6. https://doi.org/10.1109/isncc49221.2020.9297251

Dumont, D. (2010). Cyber security concerns of Supervisory Control and Data Acquisition (SCADA) systems. *2010 IEEE International Conference on Technologies for Homeland Security (HST)*, *NA*(NA), 473-475. https://doi.org/10.1109/ths.2010.5654964

Duncan, A., Creese, S., & Goldsmith, M. (2012). TrustCom - Insider Attacks in Cloud Computing. *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, *NA*(NA), 857-862. https://doi.org/10.1109/trustcom.2012.188

Efe, A., Tuzlupınar, B., & Cavlan, A. C. (2019). Air Traffic Security against Cyber Threats. *Bilge International Journal of Science and Technology Research*, *3*(2), 135-143. https://doi.org/10.30516/bilgesci.405074

Enbody, R., Sood, A. K., & Bajpai, P. (2018). *eCrime - A key-management-based taxonomy for ransomware* (Vol. NA). IEEE. https://doi.org/10.1109/ecrime.2018.8376213

Endoh, H. (2008). Analyzing aspects of cyber security standard for M&CS. *2008 SICE Annual Conference*, *NA*(NA), 1478-1481. https://doi.org/10.1109/sice.2008.4654892

Fadhil, S. A. (2021). Internet of Things security threats and key technologies. *Journal of Discrete Mathematical Sciences and Cryptography*, *24*(7), 1951-1957. https://doi.org/10.1080/09720529.2021.1957189

Falco, J. A., Scarfone, K. A., & Stouffer, K. A. (2011). Guide to Industrial Control Systems (ICS) Security:

Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations Such as Programmable Logic Controllers (PLC): Recommendations of the National Institute of Standards and Technology, Final Public Draft. *NA*, *NA*(NA), NA-NA. https://doi.org/10.6028/nist.sp.800-82

Fan, X., Kefeng, F., Wang, Y., & Ruikang, Z. (2015). *SSIC - Overview of cyber-security of industrial control system* (Vol. NA). IEEE. https://doi.org/10.1109/ssic.2015.7245324

Faris, H., Habib, M., Almomani, I., Eshtay, M., & Aljarah, I. (2020). Optimizing Extreme Learning Machines Using Chains of Salps for Efficient Android Ransomware Detection. *Applied Sciences*, *10*(11), 3706-NA. https://doi.org/10.3390/app10113706

Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., & Inácio, P. R. M. (2013). Security issues in cloud environments: a survey. *International Journal of Information Security*, *13*(2), 113-170. https://doi.org/10.1007/s10207-013-0208-7

Frank, M., Leitner, M., & Pahi, T. (2017). DASC/PiCom/DataCom/CyberSciTech - Design Considerations for Cyber Security Testbeds: A Case Study on a Cyber Security Testbed for Education. *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech)*, *NA*(NA), 38-46. https://doi.org/10.1109/dasc-picom-datacom-cyberscitec.2017.23

Gómez-Hernández, J. A., Álvarez-González, L., & García-Teodoro, P. (2018). R-Locker: Thwarting ransomware action through a honeyfile-based approach. *Computers & Security*, *73*(NA), 389-398. https://doi.org/10.1016/j.cose.2017.11.019

Gopalakrishnan, K., Govindarasu, M., Jacobson, D., & Phares, B. M. (2013). Cyber Security for Airports. *INTERNATIONAL JOURNAL FOR TRAFFIC AND TRANSPORT ENGINEERING*, *3*(4), 365-376. https://doi.org/10.7708/ijtte.2013.3(4).02

He, H., Maple, C., Watson, T., Tiwari, A., Mehnen, J., Jin, Y., & Gabrys, B. (2016). CEC - The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence. *2016 IEEE Congress on Evolutionary Computation (CEC)*, *NA*(NA), 1015-1021. https://doi.org/10.1109/cec.2016.7743900

Hirano, M., & Kobayashi, R. (2019). Machine Learning Based Ransomware Detection Using Storage Access Patterns Obtained From Live-forensic Hypervisor. *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, *NA*(NA), 1-6. https://doi.org/10.1109/iotsms48152.2019.8939214

Iwendi, C., Jalil, Z., Javed, A. R., Reddy, G. T., Kaluri, R., Srivastava, G., & Jo, O. (2020). KeySplitWatermark: Zero Watermarking Algorithm for Software Protection Against Cyber-Attacks. *IEEE Access*, *8*(NA), 72650-72660. https://doi.org/10.1109/access.2020.2988160

Jasper, S. (2016). U.S. Cyber Threat Intelligence Sharing Frameworks. *International Journal of Intelligence and CounterIntelligence*, *30*(1), 53-65. https://doi.org/10.1080/08850607.2016.1230701

Javed, A. R., Abid, R., Aslam, B., Khalid, H. A., Khan, M. Z., Alhazmi, O. H., & Rizwan, M. (2021). Green5G: Enhancing Capacity and Coverage in Device-to-Device Communication. *Computers, Materials & Continua*, *67*(2), 1933-1950. https://doi.org/10.32604/cmc.2021.015272

Javed, A. R., Beg, M. O., Asim, M., Baker, T., & Al-Bayatti, A. H. (2020). AlphaLogger: detecting motion-based side-channel attack using smartphone keystrokes. *Journal of Ambient Intelligence and Humanized Computing*, *14*(5), 4869-4882. https://doi.org/10.1007/s12652-020-01770-0

Javed, A. R., & Jalil, Z. (2020). Byte-Level Object Identification for Forensic Investigation of Digital Images. *2020 International Conference on Cyber Warfare and Security (ICCWS)*, *NA*(NA), NA-NA. https://doi.org/10.1109/iccws48432.2020.9292387

Javed, A. R., Jalil, Z., Moqurrab, S. A., Abbas, S., & Liu, X. (2020). Ensemble Adaboost classifier for accurate and fast detection of botnet attacks in connected vehicles. *Transactions on Emerging Telecommunications Technologies*, *33*(10), NA-NA. https://doi.org/10.1002/ett.4088

Javed, A. R., Rehman, S. u., Khan, M. U., Alazab, M., & G, T. R. (2021). CANintelliIDS: Detecting In-Vehicle Intrusion Attacks on a Controller Area Network Using CNN and Attention-Based GRU. *IEEE Transactions on Network Science and Engineering*, *8*(2), 1456-1466. https://doi.org/10.1109/tnse.2021.3059881

Javed, A. R., Rehman, S. u., Khan, M. U., Alazab, M., & Khan, H. U. (2021). Betalogger: Smartphone Sensor-based Side-channel Attack Detection and Text Inference Using Language Modeling and

Dense MultiLayer Neural Network. *ACM Transactions on Asian and Low-Resource Language Information Processing*, *20*(5), 1-17. https://doi.org/10.1145/3460392

Javed, A. R., Usman, M., Rehman, S. u., Khan, M. U., & Haghighi, M. S. (2021). Anomaly Detection in Automated Vehicles Using Multistage Attention-Based Convolutional Neural Network. *IEEE Transactions on Intelligent Transportation Systems*, *22*(7), 4291-4300. https://doi.org/10.1109/tits.2020.3025875

Jia, Fan, Xie, & Di. (2016). A Unified Method Based on SPA and Timing Attacks on the Improved RSA. *NA*, *NA*(4), 89-96. https://doi.org/NA

Jiang, H., Fujishiro, M., Kodera, H., Yanagisawa, M., & Togawa, N. (2015). Scan-Based Side-Channel Attack on the Camellia Block Cipher Using Scan Signatures. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, *E98.A*(12), 2547-2555. https://doi.org/10.1587/transfun.e98.a.2547

Jimenez, J. I., Jahankhani, H., & Kendzierskyj, S. (2019). Health Care in the Cyberspace: Medical Cyber-Physical System and Digital Twin Challenges. In (Vol. NA, pp. 79-92). Springer International Publishing. https://doi.org/10.1007/978-3-030-18732-3_6

Kagalwalla, N., & Churi, P. (2019). Cybersecurity in Aviation : An Intrinsic Review. *2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA)*, *NA*(NA), 1-6. https://doi.org/10.1109/iccubea47591.2019.9128483

Kanwal, M., & Thakur, S. (2017). An app based on static analysis for android ransomware. *2017 International Conference on Computing, Communication and Automation (ICCCA)*, *NA*(NA), 813-818. https://doi.org/10.1109/ccaa.2017.8229907

Kao, D.-Y., & Hsiao, S.-C. (2018). The dynamic analysis of WannaCry ransomware. *2018 20th International Conference on Advanced Communication Technology (ICACT)*, *NA*(NA), 159-166. https://doi.org/10.23919/icact.2018.8323682

Keller, J. Y., & Sauter, D. (2013). Monitoring of stealthy attack in networked control systems. *2013 Conference on Control and Fault-Tolerant Systems (SysTol)*, *NA*(NA), 462-467. https://doi.org/10.1109/systol.2013.6693850

Khan, F., Ncube, C., Kumar, R. L., Kadry, S., & Nam, Y. (2020). A Digital DNA Sequencing Engine for Ransomware Detection Using Machine Learning. *IEEE Access*, *8*(NA), 119710-119719. https://doi.org/10.1109/access.2020.3003785

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015). DIMVA - Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks. In (Vol. NA, pp. 3-24). Springer International Publishing. https://doi.org/10.1007/978-3-319-20550-2_1

Kim, D., & Lee, J.-H. (2020). Blacklist vs. Whitelist-Based Ransomware Solutions. *IEEE Consumer Electronics Magazine*, *9*(3), 22-28. https://doi.org/10.1109/mce.2019.2956192

Koroniotis, N., Moustafa, N., Schiliro, F., Gauravaram, P., & Janicke, H. (2020). A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports. *IEEE Access*, *8*(2020), 209802-209834. https://doi.org/10.1109/access.2020.3036728

Kramer, S., & Bradfield, J. C. (2009). A general definition of malware. *Journal in Computer Virology*, *6*(2), 105-114. https://doi.org/10.1007/s11416-009-0137-1

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

Lee, K., Yim, K., & Seo, J. (2017). Ransomware prevention technique using key backup: Ransomware prevention technique using key backup. *Concurrency and Computation: Practice and Experience*, *30*(3), NA-NA. https://doi.org/10.1002/cpe.4337

Lee, S., Lee, S., Yoo, H., Kwon, S., & Shon, T. (2017). Design and implementation of cybersecurity testbed for industrial IoT systems. *The Journal of Supercomputing*, *74*(9), 4506-4520. https://doi.org/10.1007/s11227-017-2219-z

Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2018). Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls. *Sensors (Basel, Switzerland)*, *19*(1), 19-NA. https://doi.org/10.3390/s19010019

McIntosh, T. R., Jang-Jaccard, J., Watters, P. A., & Susnjak, T. (2019). ICONIP (5) - The inadequacy of entropy-based ransomware detection. In (Vol. NA, pp. 181-189). Springer International Publishing. https://doi.org/10.1007/978-3-030-36802-9_20

Mehnaz, S., Mudgerikar, A., & Bertino, E. (2018). RAID - RWGuard: A Real-Time Detection System Against Cryptographic Ransomware. In (Vol. NA, pp. 114-

136). Springer International Publishing. https://doi.org/10.1007/978-3-030-00470-5_6

Mohit, P., & Biswas, G. P. (2016). Modification of Symmetric-Key DES into Efficient Asymmetric-Key DES using RSA. *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies*, *NA*(NA), 136-135. https://doi.org/10.1145/2905055.2905352

Muhammad, A., Asad, M., & Javed, A. R. (2020). Robust Early Stage Botnet Detection using Machine Learning. *2020 International Conference on Cyber Warfare and Security (ICCWS)*, *NA*(NA), 1-6. https://doi.org/10.1109/iccws48432.2020.9292395

Musa, S., Shahzad, A., & Aborujilah, A. (2013). ICUIMC - Secure security model implementation for security services and related attacks base on end-to-end, application layer and data link layer security. *Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication*, *NA*(NA), 32-38. https://doi.org/10.1145/2448556.2448588

Or-Meir, O., Nissim, N., Elovici, Y., & Rokach, L. (2019). Dynamic Malware Analysis in the Modern Era—A State of the Art Survey. *ACM Computing Surveys*, *52*(5), 88-48. https://doi.org/10.1145/3329786

Osvik, D. A., Shamir, A., & Tromer, E. (2006). CT-RSA - Cache attacks and countermeasures: the case of AES. In (Vol. NA, pp. 1-20). Springer Berlin Heidelberg. https://doi.org/10.1007/11605805_1

Oyewumi, I. A., Jillepalli, A. A., Richardson, P., Ashrafuzzaman, M., Johnson, B. K., Chakhchoukh, Y., Haney, M., Sheldon, F. T., & de Leon, D. C. (2019). ISAAC: The Idaho CPS Smart Grid Cybersecurity Testbed. *2019 IEEE Texas Power and Energy Conference (TPEC)*, *NA*(NA), 1-6. https://doi.org/10.1109/tpec.2019.8662189

Pahlevanzadeh, B., Koleini, S., & Fadilah, S. I. (2021). *ACeS - Security in IoT: Threats and Vulnerabilities, Layered Architecture, Encryption Mechanisms, Challenges and Solutions* (Vol. NA). Springer Singapore. https://doi.org/10.1007/978-981-33-6835-4_18

Palisse, A., Durand, A., Le Bouder, H., Le Guernic, C., & Lanet, J.-L. (2017). NordSec - Data Aware Defense (DaD): Towards a Generic and Practical Ransomware Countermeasure. In (Vol. 10674, pp. 192-208). Springer International Publishing. https://doi.org/10.1007/978-3-319-70290-2_12

Pont, J., Arief, B., & Hernandez-Castro, J. C. (2020). ISC - Why Current Statistical Approaches to Ransomware Detection Fail. In (Vol. NA, pp. 199-216). Springer International Publishing. https://doi.org/10.1007/978-3-030-62974-8_12

Sabharwal, S., & Sharma, S. (2019). Ransomware Attack : India issues Red Alert. *Advances in Intelligent Systems and Computing*, *7*(02), 471-484. https://doi.org/10.1007/978-981-13-7403-6_42

Scarani, V., Acín, A., Ribordy, G., & Gisin, N. (2004). Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. *Physical Review Letters*, *92*(5), 057901-057901. https://doi.org/10.1103/physrevlett.92.057901

Sigler, K. (2018). Crypto-jacking: how cyber-criminals are exploiting the crypto-currency boom. *Computer Fraud & Security*, *2018*(9), 12-14. https://doi.org/10.1016/s1361-3723(18)30086-1

Smit, D. (2015). Cyberbullying in South African and American schools : a legal comparative study. *South African Journal of Education*, *35*(2), 01-11. https://doi.org/10.15700/saje.v35n2a1076

Suciu, G., Scheianu, A., Vulpe, A., Petre, I., & Suciu, V. (2018). WorldCIST (3) - Cyber-Attacks – The Impact Over Airports Security and Prevention Modalities. In (Vol. NA, pp. 154-162). Springer International Publishing. https://doi.org/10.1007/978-3-319-77700-9_16

Taleqani, A. R., Nygard, K. E., Bridgelall, R., & Hough, J. (2018). EIT - Machine Learning Approach to Cyber Security in Aviation. *2018 IEEE International Conference on Electro/Information Technology (EIT)*, *NA*(NA), 0147-0152. https://doi.org/10.1109/eit.2018.8500165

Thomas, T., Vijayaraghavan, A. P., & Emmanuel, S. (2019). Machine Learning and Cybersecurity. In (Vol. NA, pp. 37-47). Springer Singapore. https://doi.org/10.1007/978-981-15-1706-8_3

Tianliang, L., Zhang, L., Wang, S., & Qi, G. (2017). *SPAC - Ransomware detection based on V-detector negative selection algorithm* (Vol. NA). IEEE. https://doi.org/10.1109/spac.2017.8304335

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

Toth, P., & Klein, P. (2014). A Role-Based Model for Federal Information Technology/Cybersecurity Training (3rd Draft). *NA*, *NA*(NA), NA-NA. https://doi.org/NA

Tsiknas, K., Taketzis, D., Demertzis, K., & Skianis, C. (2021). Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures. *IoT*, *2*(1), 163-186. https://doi.org/10.3390/iot2010009

Ugwoke, F. N., Okafor, K. C., & Chijindu, V. C. (2015). Security QoS profiling against cyber terrorism in airport network systems. *2015 International Conference on Cyberspace (CYBER-Abuja)*, *NA*(NA), 241-251. https://doi.org/10.1109/cyber-abuja.2015.7360516

Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I., & Bellekens, X. (2022). Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. *Information*, *13*(3), 146. https://doi.org/10.3390/info13030146

Valluri, M. R. (2012). Authentication Schemes Using Polynomials Over Non-Commutative Rings. *International Journal on Cryptography and Information Security*, *2*(4), 51-58. https://doi.org/10.5121/ijcis.2012.2406

von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*(NA), 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Wagner, T. D., Palomar, E., Mahbub, K., & Abdallah, A. E. (2018). A Novel Trust Taxonomy for Shared Cyber Threat Intelligence. *Security and Communication Networks*, *2018*(NA), 1-11. https://doi.org/10.1155/2018/9634507

Wang, W., & Lu, Z. (2013). Survey Cyber security in the Smart Grid: Survey and challenges. *Computer Networks*, *57*(5), 1344-1371. https://doi.org/10.1016/j.comnet.2012.12.017

Wang, X., Yu, G., Zha, X., Ni, W., Liu, R. P., Guo, Y. J., Zheng, K., & Niu, X. (2019). Capacity of Blockchain based Internet-of-Things: Testbed and Analysis. *Internet of Things*, *8*(NA), 100109-NA. https://doi.org/10.1016/j.iot.2019.100109

Wani, A., & Revathi, S. (2020). Ransomware protection in IoT using software defined networking. *International Journal of Electrical and Computer Engineering (IJECE)*, *10*(3), 3166-3175. https://doi.org/10.11591/ijece.v10i3.pp3166-3175

Wani, A. R., Rana, Q. P., & Pandey, N. (2018). Analysis and Countermeasures for Security and Privacy Issues in Cloud Computing. In (Vol. NA, pp. 47-54). Springer Singapore. https://doi.org/10.1007/978-981-10-7323-6_4

Ward, S., O'Brien, J., Beresh, B., Benmouyal, G., Holstein, D., Tengdin, J. T., Fodero, K., Simon, M., Carden, M., Yalla, M., Tibbals, T., Skendzic, V., Mix, S., Young, R., Sidhu, T., Klein, S., Weiss, J., Apostolov, A., Bui, D. P., . . . Seifert, G. (2007). Cyber Security Issues for Protective Relays; C1 Working Group Members of Power System Relaying Committee. *2007 IEEE Power Engineering Society General Meeting*, *NA*(NA), 1-8. https://doi.org/10.1109/pes.2007.385583

Weckstén, M., Frick, J., Sjostrom, A., & Järpe, E. (2016). A novel method for recovery from Crypto Ransomware infections. *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, *NA*(NA), 1354-1358. https://doi.org/10.1109/compcomm.2016.7924925

Wei, Y., Rong, Y., & Fan, C. (2018). Differential Fault Attacks on Lightweight Cipher LBlock. *Fundamenta Informaticae*, *157*(1-2), 125-139. https://doi.org/10.3233/fi-2018-1621

Weiss, J. W. (2010). *Protecting Industrial Control Systems from Electronic Threats* (Vol. NA). NA. https://doi.org/NA

Wheelus, C., & Zhu, X. (2020). IoT Network Security: Threats, Risks, and a Data-Driven Defense Framework. *IoT*, *1*(2), 259-285. https://doi.org/10.3390/iot1020016

Wu, M., Lu, T., Ling, F.-Y., Sun, J., & Du, H. (2010). Research on the architecture of Internet of Things. *2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE)*, *5*(NA), NA-NA. https://doi.org/10.1109/icacte.2010.5579493

Yadav, G., & Paul, K. (2021). Architecture and Security of SCADA Systems: A Review. *International Journal of Critical Infrastructure Protection*, *34*(NA), 100433-NA. https://doi.org/10.1016/j.ijcip.2021.100433

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