Law, Economics and Society; Vol. 1, No. 1; 2025
ISSN 3066-9340 E-ISSN 3066-9359
https://doi.org/10.30560/les.v1n1p115

Cybersecurity Regulations and Risk Management in the Financial Sector: A Comparative Analysis

Ebone McCoy[1]

[1] Capitol Technology University, Maryland, USA

Correspondence: Ebone McCoy, Capitol Technology University, Maryland, USA. E-mail: emccoy@captechu.edu

Received: February 19, 2025 Accepted: February 26, 2025 Online Published: March 23, 2025

Abstract

The financial sector has become a prime target for cyber attackers seeking unauthorized access to sensitive data. As social engineering techniques like phishing and denial of service attacks continue to escalate, greater oversight is required to secure financial institutions. While federal and state regulations in countries such as the United States and the United Kingdom aim to provide consumer protection, the level of cybersecurity implementation varies across nations. This paper explores the regulatory landscape of the financial sector, focusing on the United States, the United Kingdom, and the European Union. It examines the specific protections provided by legislation, such as the Gramm-Leach-Bliley Act, the Sarbanes-Oxley Act, and the General Data Protection Regulation. The study highlights the challenges posed by inconsistent state-level policies and the need for international cooperation to address the growing cyber-attack threat. Furthermore, it emphasizes balancing cybersecurity decision-making and policy implementation to ensure adequate regulation and social freedom. This paper also discusses the critical role of business continuity plans, disaster recovery plans, intrusion detection and prevention systems, and incident response plans in mitigating cyber risks. Finally, it explores the potential of cloud computing as a future research direction for enhancing the security and resilience of the financial sector. This review explores cybersecurity frameworks, risk assessment methodologies, and technological advancements, including cloud computing and intrusion detection systems, to mitigate cyber risks in financial institutions.

Keywords: cybersecurity, financial sector, regulations, risk management, cyber threats, data protection, cloud computing, intrusion detection systems

1. Introduction

The financial sector has become a primary target for malicious actors seeking unauthorized access to consumers' private information. The financial industry has experienced relatively more cyber-attacks by hackers post-COVID-19 (World Bank, 2021). According to the Congress Research Center, cyber threats pose operational, reputational, and systemic risks to the banking systems (Scott & Tierno, 2023). The continuous escalation in social engineering techniques, such as phishing and denial of service attacks against financial institutions, necessitates increased oversight and security measures (First Bank & Trust Company, 2025). Federal and state regulations have attempted to protect consumers with varying degrees of efficacy. The United States and the United Kingdom have implemented specific regulatory initiatives, enforced through a combination of federal and state laws, designed to safeguard consumer data and maintain the integrity of financial services (Scott & Tierno, 2023). Multiple laws and agencies regulate cybersecurity, but the system is fragmented.

These regulations aim to establish standardized security protocols and incident response procedures across financial institutions. However, the rapidly evolving nature of cyber threats often outpaces regulatory updates, creating potential vulnerabilities. To address this challenge, many financial institutions are adopting proactive approaches, including advanced threat detection systems and regular security audits, to enhance their cybersecurity posture beyond minimum regulatory requirements (Kost, 2025). Cybersecurity in finance is the countermeasures and technologies that protect financial institutions from cyber threats such as hacking, phishing, ransomware, and data breaches (Nesterenko, 2024). Proper cybersecurity measures ensure the safety of banking systems transactions, eliminating unauthorized access and cyber-attacks.

1.1 Problem Statement

The financial sector experiences one of the highest rates of breaches due to the value of financial data (Verizon, 2024). According to IBM 2024, the cost of a data breach report for the finance industry experienced the average highest cost of data breaches at $6.08 million; this is an increase from the 2023 report of $5.17 million per incident

(Ponemon Institute & IBM, 2024). Approximately 34% of individuals reported experiencing cybersecurity incidents, such as fraudulent financial transactions, unauthorized access to their online accounts, or attempts to open credit lines in their names (McClain et al., 2023). According to the Pew Research Center, institutions struggle to implement comprehensive cybersecurity strategies that are both regulation-compliant and technologically advanced to meet consumer expectations, leading consumers to believe they have little to no control over their personal information (McClain et al., 2023).

1.2 Purpose

This study investigates the financial sector's cybersecurity landscape by analyzing regulatory frameworks, risk management strategies, and technological advancements aimed at mitigating cyber threats. Considering the increasing frequency of cyber-attacks, financial institutions encounter significant challenges in safeguarding sensitive consumer data while adhering to evolving privacy legislation (Scott & Tierno, 2023). The research examines cybersecurity measures across the United States, the United Kingdom, and the European Union, elucidating data protection, consumer privacy, and regulatory enforcement approaches. This study provides insights into enhancing cybersecurity resilience within the financial sector by assessing cybersecurity frameworks, business continuity strategies, and emerging technologies such as cloud computing and artificial intelligence.

1.3 Research Question Guiding the Review Process

What are the current cybersecurity policies and risk management strategies implemented in financial institutions across the United States, the United Kingdom, and the European Union, and how do technological advancements influence their effectiveness in mitigating cyber threats?

2. Method

The study employed a rapid literature review. A rapid literature review (RLR) is a streamlined approach to synthesizing existing research evidence within a condensed timeframe, balancing methodological rigor with efficiency. Its value is providing timely, evidence-based insights to inform decision-making, particularly in dynamic contexts such as public health emergencies, policy development, and clinical practice guidelines. Unlike traditional systematic reviews, RLRs apply methodological shortcuts, such as limiting search databases, restricting publication dates, or narrowing inclusion criteria, to expedite the review process while maintaining sufficient credibility and reliability (Smela et al., 2023)

2.1 Search Strategy

A rapid literature review methodology addressed this research question, focusing on peer-reviewed academic articles, industry reports, and regulatory documents related to cybersecurity in the financial sector. Key databases utilized included Research Gate, Academia.edu, ProQuest, Scopus, IGI Publishing, ScienceDirect, JSTOR, DOAJ, and Google Scholar to capture a broad spectrum of interdisciplinary insights.

2.2 Key Search Terms

The search incorporated a combination of keywords and Boolean operators to enhance the precision and relevance of results. The primary search terms included:

- "Cybersecurity policies" AND "financial institutions"
- "Risk management strategies" AND "cyber threats"
- "Data protection regulations" OR "financial sector compliance"
- "Cloud forensics" OR "intrusion detection systems" OR "AI-driven security solutions"
- "Regulatory frameworks" AND "United States" AND "United Kingdom" AND "European Union"

Boolean operators such as AND, OR, and NOT were employed to refine the search, ensuring comprehensive coverage while excluding irrelevant studies.

Inclusion Criteria:

Studies were included based on the following criteria:

1. Published between 2015 and 2024 to ensure contemporary relevance.
2. Focused on cybersecurity regulations, risk management strategies, or technological advancements relevant to the financial sector.
3. Comparative studies examining regulatory frameworks in the United States, the United Kingdom, and the European Union.

4. Peer-reviewed journal articles, government reports, industry white papers, and credible cybersecurity conference proceedings.

2.3 Review Process

The initial search yielded over 207 articles, screened for relevance through title and abstract review. Full-text analysis was conducted on 44 selected studies to extract data on cybersecurity practices, regulatory approaches, and the integration of emerging technologies such as cloud forensics, intrusion detection systems, and theories. A comparative analysis highlighted key differences in data protection philosophies, enforcement mechanisms, and the role of technology in enhancing cybersecurity resilience across jurisdictions.

3. Literature Review

3.1 Reason's Swiss Cheese Model

In financial institutions, cyber defense layers include administrative policies, technical controls (firewalls, IDS/IPS), and user behavior. Reason's Swiss Cheese Model of Accident Causation is highly applicable to understanding cybersecurity breaches in large, complex organizations (Ebert et al., 2023). The model conceptualizes an organization's defenses as multiple layers of protective barriers, each represented by a slice of Swiss cheese (Ebert et al., 2023). These barriers include technical controls like firewalls and intrusion detection systems, administrative measures such as security policies and protocols, and human elements like employee awareness and training. Each layer is intended to prevent threats from penetrating the organization's defenses. However, these layers are not flawless; they contain inherent vulnerabilities or "holes" due to outdated software, poor security practices, human error, or insufficient policy enforcement (Ebert et al., 2023). A cybersecurity breach occurs when these holes momentarily align across multiple layers, creating a pathway that allows threats to bypass all defenses and compromise sensitive systems or data (Ebert et al., 2023).

In large organizations, the complexity and scale of operations increase the likelihood of such vulnerabilities existing simultaneously across different layers. For example, a sophisticated phishing attack might exploit gaps in employee training (human layer), weaknesses in email filtering technology (technical layer), and inadequate incident response procedures (organizational layer). The Swiss Cheese Model highlights the importance of a defense-in-depth strategy, where multiple, overlapping layers of security reduce the probability of a single point of failure leading to a breach. It also emphasizes the dynamic nature of these vulnerabilities, as organizational changes, evolving threat landscapes, and human behaviors continually create new "holes" that require constant monitoring, adaptation, and reinforcement of cybersecurity measures (Ebert et al., 2023).

3.2 Cognitive Load Theory (CLT)

Cognitive Load Theory (CLT) explores the mental effort required to process, understand, and apply information, making it particularly relevant in cybersecurity within financial institutions (Bernard et al., 2021; Raywood-Burke, 2023). Cybersecurity protocols are often intricate, involving multiple layers of authentication, complex password requirements, and various procedural steps to ensure data security. For employees, especially those without specialized IT backgrounds, navigating these protocols can create a significant cognitive load, leading to confusion, errors, and even security breaches. For instance, an employee tasked with following a complicated multi-step verification process under the stress of tight deadlines may inadvertently skip critical security checks, exposing the system to potential threats.

The cognitive load becomes even more pronounced in high-stress environments where quick decision-making is essential. Consider a scenario where an employee receives an urgent email appearing to be from a senior executive requesting sensitive financial data. The pressure to respond quickly, combined with the mental effort required to verify the email's authenticity against complex cybersecurity guidelines, can overwhelm the employee's cognitive resources. This mental overload increases the risk of falling victim to phishing attacks, as the employee may overlook subtle red flags, such as slight discrepancies in the sender's address or unusual language patterns (Bernard et al., 2021; Raywood-Burke, 2023). The cognitive strain diminishes their ability to apply critical thinking effectively, resulting in compromised security.

To mitigate these risks, financial institutions can apply CLT principles by simplifying cybersecurity protocols and reducing unnecessary complexity in their systems. This involves designing user-friendly interfaces that guide employees intuitively through security procedures without requiring them to remember numerous intricate steps. For example, implementing single sign-on systems or adaptive security measures that automatically adjust based on user behavior can significantly reduce cognitive load. Additionally, providing concise, targeted cybersecurity training focusing on key threat indicators and practical response strategies helps employees process and retain critical information more efficiently. By aligning cybersecurity practices with the cognitive capabilities of their

workforce, organizations can enhance security compliance while minimizing the likelihood of human error (Bernard et al., 2021; Raywood-Burke, 2023).

3.3 Shell's Scenario Planning Model

Shell's Scenario Planning Model is a strategic framework that enables financial institutions to anticipate and prepare for various future cybersecurity scenarios, thereby enhancing their resilience against potential threats (Veerasamy, 2019). This model encourages organizations to move beyond reactive security measures and adopt a proactive approach by imagining multiple plausible futures. For instance, a financial institution might develop scenarios that explore the consequences of a major data breach caused by a sophisticated ransomware attack, a regulatory overhaul mandating stricter data protection measures, or a technological breakthrough that renders current encryption methods obsolete. By considering these varied possibilities, organizations can identify vulnerabilities within their current cybersecurity infrastructure and devise strategies to address them before actual threats materialize.

The model's strength lies in its ability to accommodate the inherent uncertainty of the cybersecurity landscape, where threats evolve rapidly, and new risks can emerge unexpectedly (Veerasamy, 2019). Consider a scenario where a financial institution envisions a worse-case future in which state-sponsored cyber-attacks become more frequent, targeting critical financial infrastructure. The institution might identify weaknesses in its incident response protocols, supply chain security, or international data transfer policies by exploring this scenario. This foresight enables the development of contingency plans, such as establishing partnerships with cybersecurity firms specializing in threat intelligence, investing in advanced intrusion detection systems, or conducting regular security audits focused on geopolitical risk factors. Through this process, organizations are better prepared to respond swiftly and effectively to emerging threats, reducing the potential impact on their operations and reputation.

Furthermore, Shell's Scenario Planning Model fosters a culture of strategic thinking and adaptability within financial institutions, encouraging leaders to consider cybersecurity not just as an IT issue but as an integral component of enterprise risk management (Veerasamy, 2019). For example, a financial institution might simulate a scenario where consumer trust plummets following a high-profile data breach in the industry, even though the breach did not directly affect their organization. This exercise could reveal gaps in the institution's communication strategy, leading to the development of comprehensive crisis management plans, including transparent customer outreach, media response protocols, and internal coordination mechanisms. By regularly engaging in scenario planning exercises, financial institutions can stay ahead of evolving cyber threats, ensuring that their security strategies remain robust, flexible, and aligned with both current risks and future uncertainties.

3.4 Monte Carlo Risk Analysis

Monte Carlo Risk Analysis is a powerful quantitative risk assessment tool that leverages statistical simulations to predict the likelihood of various outcomes under uncertain conditions (Fagade et al., 2017; Ncubukezi, 2020). In cybersecurity, particularly within the financial sector, this method proves invaluable in modeling the potential impact of cyber incidents such as data breaches, ransomware attacks, and denial-of-service disruptions. By running thousands of simulations with varying inputs, such as the frequency of cyber-attacks, the severity of potential breaches, and the effectiveness of security controls, financial institutions can gain a probabilistic understanding of how different cyber events might unfold (Fagade et al., 2017; Ncubukezi, 2020). This statistical approach moves beyond simple risk identification, offering detailed projections on financial losses, recovery timelines, and the cascading effects on business operations (Fagade et al., 2017; Ncubukezi, 2020).

For example, a financial institution concerned about the risk of a large-scale data breach could use Monte Carlo simulations to evaluate different attack scenarios. The analysis might consider factors such as the number of compromised records, regulatory fines, legal costs, and reputational damage. By inputting historical data and expert assumptions into the simulation, the institution can generate a range of possible outcomes, from minor breaches with minimal financial consequences to catastrophic incidents resulting in multimillion-dollar losses. This process helps decision-makers understand the average potential loss and the full spectrum of risks, including worst-case scenarios that could severely impact the organization's financial stability (Fagade et al., 2017; Ncubukezi, 2020). Armed with this knowledge, the institution can make informed decisions about where to allocate cybersecurity resources most effectively, such as investing in advanced threat detection systems, employee training programs, or enhanced encryption technologies.

Moreover, Monte Carlo Risk Analysis supports dynamic, data-driven risk management strategies that evolve with the cybersecurity landscape (Fagade et al., 2017; Ncubukezi, 2020). As new threats emerge and regulatory environments shift, financial institutions can continuously update their simulations with the latest data, allowing for real-time risk assessments. For instance, an organization might revise its models after an industry-wide

ransomware surge to reflect higher attack probabilities and more sophisticated threat vectors. This iterative approach enables institutions to remain agile, proactively adjusting their cybersecurity postures and business continuity plans in response to changing risk profiles. Ultimately, Monte Carlo Risk Analysis quantifies the financial implications of cyber threats and fosters a culture of proactive, evidence-based decision-making that strengthens an organization's overall resilience against cybersecurity risks (Fagade et al., 2017; Ncubukezi, 2020).

3.5 Socio-Technical Systems (STS) Theory

Socio-Technical Systems (STS) Theory highlights the interconnectedness of people, technology, and organizational structures, underscoring that these elements must function harmoniously to achieve optimal system performance (Malatji et al., 2019; Malatji et al., 2020). In the context of cybersecurity within financial institutions, this theory illustrates that robust security cannot rely solely on technical defenses such as firewalls, encryption, or intrusion detection systems. Instead, cybersecurity must be viewed as a dynamic system where human behavior, technological infrastructure, and organizational policies are interdependent (Malatji et al., 2019; Malatji et al., 2020). For example, even the most sophisticated security software can be ineffective if employees are unaware of phishing threats or fail to adhere to security protocols. Thus, STS Theory encourages organizations to develop cybersecurity strategies that integrate both technical solutions and human factors, creating a more resilient security posture (Malatji et al., 2019; Malatji et al., 2020).

Consider a scenario in which a financial institution experiences a data breach not because of a technological failure but due to a social engineering attack that exploited an employee's lack of cybersecurity awareness. While the institution may have had state-of-the-art security systems, the breach occurred because the organizational culture did not prioritize ongoing security training and awareness programs. This example illustrates how gaps in communication, insufficient employee training, or lack of leadership engagement can create vulnerabilities as significant as technical flaws. STS Theory emphasizes that addressing cybersecurity risks requires a holistic approach, where continuous employee education, clear communication of security policies, and a culture of accountability are integral parts of the security ecosystem (Malatji et al., 2019; Malatji et al., 2020).

Furthermore, STS Theory promotes the idea that effective cybersecurity governance relies on leadership commitment to fostering a security-conscious organizational environment (Malatji et al., 2019; Malatji et al., 2020). Leadership plays a pivotal role in setting the tone for cybersecurity practices, influencing both policy development and employee behavior. For instance, executives actively participate in cybersecurity initiatives, such as attending security briefings, supporting investment in advanced security technologies, and championing organization-wide training programs. These approaches reinforce the importance of cybersecurity at every level of the institution. This leadership involvement helps bridge the gap between technical teams and non-technical staff, ensuring that cybersecurity is not merely an IT issue but a critical organizational priority (Malatji et al., 2019; Malatji et al., 2020). By aligning technological capabilities with human behaviors and governance structures, STS Theory provides a comprehensive framework for building resilient cybersecurity systems in the financial sector.

3.6 Real Options Theory

Real Options Theory provides a dynamic framework for decision-making in cybersecurity investments by viewing these decisions as flexible opportunities rather than rigid, one-time commitments (Benaroch, 2018; Gordon et al., 2015). This perspective is particularly valuable in the rapidly evolving cybersecurity landscape where financial institutions face constantly changing threats and regulatory environments. Unlike traditional investment models focusing on fixed, long-term strategies, Real Options Theory allows organizations to make incremental investments, evaluate outcomes, and adjust their cybersecurity posture as new risks emerge (Benaroch, 2018; Gordon et al., 2015). This adaptability is critical in cybersecurity, where technologies and threat vectors evolve faster than many organizations can predict, making static security models obsolete almost as soon as they are implemented.

Consider a financial institution contemplating an investment in cloud security infrastructure. Instead of committing extensive resources to a comprehensive, inflexible system upfront, the organization could adopt a scalable cloud security solution, treating this investment as a "real option" (Benaroch, 2018; Gordon et al., 2015). As new cybersecurity threats are identified or regulatory requirements change, the institution can expand, modify, or even abandon specific security measures without incurring prohibitive costs. For instance, if the financial sector faces a sudden surge in ransomware attacks targeting cloud environments, the organization can swiftly enhance its security protocols, such as adding advanced threat detection tools or multi-factor authentication, without overhauling the entire system. This strategic flexibility reduces financial risk while maintaining a strong security posture.

Moreover, Real Options Theory supports proactive risk management by encouraging organizations to view

cybersecurity investments as opportunities to create value rather than costs to mitigate threats (Benaroch, 2018; Gordon et al., 2015). For example, an institution might pilot a new AI-driven threat detection system within a specific business unit. This pilot acts as an exploratory option, providing valuable data on the system's effectiveness before scaling it organization-wide. If the system proves effective in identifying and mitigating threats, the institution can exercise the option to expand its implementation, maximizing the return on investment. Conversely, the institution can pivot to alternative solutions with minimal sunk costs if the technology falls short. This strategic approach aligns cybersecurity investments with organizational growth, ensuring security measures evolve alongside business objectives and external risk factors (Benaroch, 2018; Gordon et al., 2015).

3.7 Complex Adaptive Systems (CAS)

Complex Adaptive Systems (CAS) Theory offers a valuable framework for understanding the dynamic and interconnected nature of financial institutions, particularly when it comes to cybersecurity (Koola, 2018). Financial institutions operate within ecosystems where technology, people, regulatory frameworks, and external threats are interdependent, constantly interacting, and evolving. CAS Theory suggests that rigid, one-size-fits-all cybersecurity strategies are ineffective in such environments because threats and vulnerabilities are not static (Koola, 2018). Instead, organizations must adopt adaptive security measures that can evolve in response to internal changes, such as new business processes, and external factors, like emerging cyber threats or shifts in regulatory requirements. This view reframes cybersecurity not just as a technical challenge but as an ongoing process of adaptation and learning (Koola, 2018).

Consider a financial institution facing the rapid emergence of sophisticated phishing attacks that exploit new social engineering tactics. A traditional security model might rely heavily on static defenses, such as fixed firewall configurations or standardized employee training modules, quickly becoming outdated as attackers evolve their methods. In contrast, by applying CAS Theory, the institution would recognize the need for flexible, responsive security strategies. This could involve implementing machine learning algorithms to identify new phishing patterns in real time alongside adaptive employee training programs that evolve based on the latest threat intelligence. The ability to dynamically adjust defenses in response to changes in the threat landscape exemplifies the core CAS principle of continuous adaptation (Koola, 2018).

Furthermore, CAS Theory emphasizes resilience as a critical component of cybersecurity, viewing it as the capacity to absorb shocks, recover from disruptions, and even thrive in adversity (Koola, 2018). For example, when a financial institution experiences a data breach, a CAS-informed approach focuses not only on immediate incident response but also on how the organization learns from the event to improve future security. This might involve conducting thorough post-incident analyses, fostering cross-functional collaboration to identify systemic vulnerabilities, and continuously refining security protocols based on lessons learned. By embracing the principles of resilience, flexibility, and continuous learning, financial institutions can develop cybersecurity strategies that are reactive and proactive, capable of withstanding and adapting to the ever-evolving landscape of cyber threats.

3.8 Cyber Security Regulations and Financial Oversight in the United States

The United States (US) instituted many protections against public and private entities with access to consumer financial information. There is no comprehensive law regulating cybersecurity in the United States; various laws and agencies govern financial cybersecurity (Scott & Tierno, 2023). Privacy laws are central to financial institutions due to Legislative efforts such as the Gramm-Leach-Bliley Act (GLBA) and Sarbanes-Oxley (SOX) Act. These regulations protect consumers by developing procedures for companies to manage consumer information properly (Kost, 2025). According to the Federal Trade Commission, under the GBLA, financial institutions offering services such as loans or insurance must disclose their information-sharing practices to customers and outline the measures implemented to protect customer data (Federal Trade Commission, n.d.). The Sarbanes-Oxley (SOX) Act mandates security controls to protect financial data integrity and is mandatory for all public companies, including those in the financial sector (De Groot, 2024). Compliance with these regulations involves regular assessments, internal and external audits, and establishing business continuity (Kost, 2025).

In general, all states across the US provide mandatory explicit consent to share customer data and mandatory company disclosures when a breach occurs. However, many states fail to provide further protections for residents, such as laws protecting biometric data (McClain et al., 2023).

California has the nation's strictest privacy and data protection laws and passed the Consumer Privacy Act of 2018. This act gives consumers the right to understand what data any organization has gathered about them and with whom that data is being shared. This gives consumers control over their data, including the ability to delete personal data the company has collected on them (Bischoff, 2023).

3.9 Cybersecurity Regulations and Financial Oversight in the United Kingdom

The United Kingdom (UK) has established comprehensive cybersecurity regulations to safeguard consumer data (Kost, 2025). One of the primary legislative instruments governing data protection is the UK General Data Protection Regulation (UK-GDPR), which applies to all businesses that collect and process the personal data of UK residents. The UK-GDPR closely aligns with the European Union's General Data Protection Regulation (EU-GDPR) but includes specific modifications to reflect domestic legislative requirements (Kuner et al., 2020). Compliance with UK-GDPR mandates that organizations implement robust security measures, maintain transparency in data processing, and ensure that individuals' rights concerning their data are upheld (Information Commissioner's Office, 2023).

The **Financial Conduct Authority (FCA)** plays a crucial role in ensuring data protection and market integrity. Established under the Financial Services and Markets Act (FSMA) of 2000, the FCA enforces regulatory compliance within financial institutions, aligning its policies with European and international cybersecurity standards (Financial Conduct Authority, 2024). In addition to the FCA, the **Prudential Regulation Authority (PRA)** and the **Financial Ombudsman Service (FOS)** contribute to the broader financial regulatory framework. The PRA focuses on the resilience of banks, insurance firms, and investment companies, ensuring they manage risks effectively, including cybersecurity threats (Bank of England, 2023). The FOS provides an avenue for consumers to seek redress in cases of financial misconduct, including breaches involving personal data security (Kost, 2025).

3.10 GDPR vs US Data Protection/Differences in Data Protection Philosophy

The GDPR represents a comprehensive framework for generalized control and regulation of personal data protection with the European Union. The European Union's primary goal is to supersede any contradictory laws that exist at the national level to regulate data protection precisely, empowering individuals to control their data. (Bakare et al., 2024). In contrast, the United States aims to preserve data integrity as a commercial asset. The regulatory landscape of the US is comprised of various sector-specific laws, creating a varied approach to data protection and individual privacy compared to the GDPR (Bakare et al., 2024). Despite the differences, the shared goal of protecting data and privacy highlights the need for collaboration between the EU and the US.

The EU-US Privacy Shield Framework was established to facilitate intercontinental exchanges of personal data for commercial purposes, promoting compliance and cooperation between the two parties (Bakare et al., 2024). US businesses that engage with EU entities are under strict regulatory oversight and face penalties, including fines, for violating the privacy standards set forth by the Privacy Shield agreement. (Minssen et al., 2020). Although this framework aimed to balance US business operability and EU data protection standards, it fails to encompass all rights guaranteed by the GDPR, such as specific individual privacy rights.

3.11 Cyber Security Frameworks

The UK banks maintain significant autonomy in assessing cybersecurity as part of ongoing risk-based supervisory activities. One such framework is CBEST, a threat intelligence-led cybersecurity testing framework (Bank of England, 2021). The UK's CBEST framework provides a timeline that banks follow in simulating a cyber-attack. The framework is divided into four phases that demonstrate the guidance in intelligence gathering and attack methods, culminating in a remediation plan provided to the bank. Figure 1 is a visual of the CBEST framework.

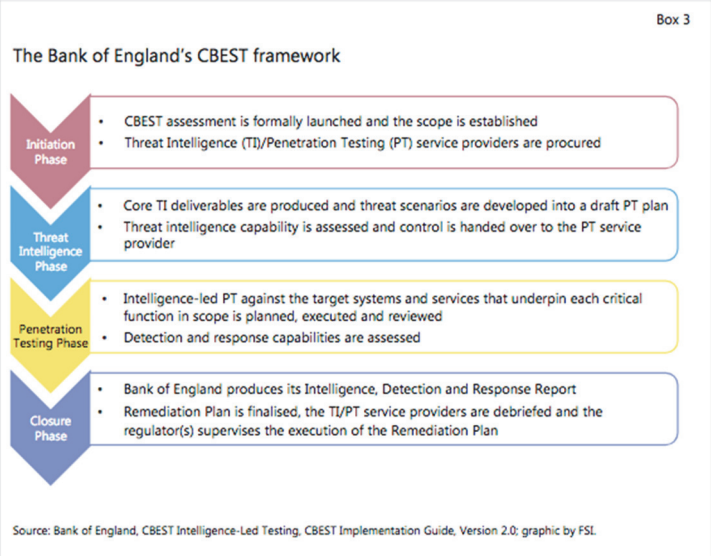

Figure 1. Framework for England's CBEST program

The National Institute of Standards and Technology has issued SP 800-94 to guide financial sectors in characterizing their intrusion detection and prevention software (IDPS) to protect their critical infrastructure. IDPS technology monitors network activity for malicious traffic and mitigates potential threats (Kennedy & Joseph, 2024).

3.12 Cybersecurity Risk Management

Cyber-attacks on the financial sector have increased over the last three years, with 65% of American customers experiencing more cyber threats than those in other industries (World Economic Forum, 2025). Addressing these risks requires effective cybersecurity decision-making guided by well-defined cyber policies. Cyber policy regulates digital data exchange, including internet usage and cyber defense (Utica University, 2019). A balanced approach between regulation and operational freedom is essential to ensure strong cybersecurity while maintaining efficiency in financial operations. The financial industry faces various cyber-attack vectors, including phishing, Denial of Service (DDoS), ransomware, and insider attacks. These threats pose significant risks to financial institutions and their customers, leading to data breaches, financial losses, and reputational damage (Darem et al., 2023).

3.13 Phishing Attacks

Social engineering attacks have become increasingly sophisticated, targeting not only technological vulnerabilities but also the human element within organizations, especially in the financial sector. Phishing, one of the most common forms, manipulates individuals into disclosing sensitive information through deceptive emails that seem to come from trusted sources. For instance, an employee at a financial institution might receive an urgent email that appears to be from their IT department, urging them to reset their password due to a security breach. The email includes a malicious link that directs the user to a fake website, capturing their login credentials. According to Verizon (2024), phishing attacks continue to dominate the threat landscape in the financial industry, exploiting employees' natural inclination to trust authority and react quickly to urgent requests. These attacks are especially effective because they exploit human emotions like fear, curiosity, or the desire to be helpful, making technical defenses inadequate without strong employee awareness and training programs.

Spear phishing takes this threat further by targeting specific individuals within an organization, often using personal information gleaned from social media or data breaches to craft persuasive messages. For instance, a senior financial analyst might receive an email referencing a recent industry conference they attended, complete with details about the event and an attachment labeled "conference materials." Believing the email to be legitimate, the analyst opens the attachment, inadvertently downloading malware that compromises the organization's network. The challenge with spear phishing is its personalized nature, which makes it difficult to detect using standard security filters. Business Email Compromise (BEC) attacks, a sophisticated form of spear phishing, exploit compromised or spoofed executive email accounts to authorize fraudulent transactions. Verizon (2024) highlights the growing financial impact of BEC attacks, as cybercriminals convincingly impersonate C-suite

executives, instructing finance teams to transfer large sums of money to offshore accounts under the guise of confidential business deals.

Whaling, another variant of social engineering, specifically targets high-ranking executives or individuals with privileged access to sensitive financial data. These attacks often involve meticulously researched emails that mimic legitimate business correspondence, making them exceptionally difficult to detect. For example, a CEO of a multinational bank might receive an email purportedly from a board member requesting approval for an urgent wire transfer related to a confidential acquisition. The email could contain official logos and industry-specific jargon and even appear to come from a familiar contact, increasing its credibility. The complexities of defending against such attacks lie in the attackers' ability to blend into the organization's communication patterns, bypassing traditional security measures. As social engineering tactics evolve, financial institutions face the dual challenge of implementing advanced technical defenses while fostering a security-conscious culture through continuous employee education, simulated phishing exercises, and strong incident response protocols.

3.14 Denial of Service (DDoS) Attacks

Denial of Service (DDoS) attacks are a pervasive and evolving threat to financial institutions, designed to overwhelm systems with excessive traffic, rendering critical services inaccessible to legitimate users. These attacks flood networks, servers, or applications with massive amounts of data requests, often originating from a distributed network of compromised devices known as botnets. For example, a major financial institution could experience a sudden surge of fraudulent traffic targeting its online banking platform, overwhelming the server's capacity and causing the system to crash. Customers cannot perform essential transactions such as fund transfers, bill payments, or access account information during an outage. According to Verizon (2024), these disruptions erode customer trust and lead to direct financial losses, as the downtime can cost institutions thousands of dollars per hour in lost revenue, recovery expenses, and reputational damage.

The challenges posed by DDoS attacks extend beyond immediate service disruptions, as attackers increasingly employ sophisticated techniques that complicate detection and mitigation. Unlike traditional attacks that rely on a single vector, modern DDoS campaigns often involve multi-vector strategies, simultaneously targeting different layers of an organization's infrastructure. For instance, an attack might simultaneously flood the network with massive traffic (volumetric attack), exploit vulnerabilities in application protocols (protocol attack), and target specific web applications with crafted requests (application-layer attack). This complexity makes it difficult for standard security measures to identify and filter out malicious traffic without affecting legitimate users. Financial institutions, relying on real-time transactions and stringent uptime requirements, face the additional burden of balancing robust security measures with seamless user experiences, often requiring deploying advanced DDoS mitigation services and traffic analysis tools to respond effectively (Razavi et al., 2023).

The impact of DDoS attacks on financial institutions is not limited to technical or operational setbacks; they also have significant legal, regulatory, and reputational implications. For example, suppose a prolonged DDoS attack disrupts services at a major bank. In that case, regulators may scrutinize the institution's cybersecurity resilience and incident response capabilities, potentially leading to fines or mandatory corrective actions. Additionally, attackers often use DDoS assaults as a smokescreen for more targeted cybercrimes, such as data breaches or financial fraud, diverting the attention of security teams while executing more covert operations. The financial sector's interconnected nature further exacerbates the risk, as a successful attack on one institution can ripple across payment systems, stock exchanges, and third-party service providers. To counter these threats, financial institutions must invest in layered security architectures, real-time threat intelligence sharing, and comprehensive incident response plans that include DDoS-specific contingencies, ensuring both rapid detection and swift mitigation in the face of increasingly complex cyber threats (Verizon, 2024; Razavi et al., 2023).

3.15 Insider Attacks

Insider threats in cybersecurity are particularly insidious because they originate from individuals who already possess legitimate access to an organization's systems, such as employees, contractors, or business partners. These threats can be malicious, where an individual intentionally seeks to cause harm, or unintentional, stemming from negligence or lack of awareness. For instance, a disgruntled employee with administrative privileges might deliberately exfiltrate sensitive financial data to sell on the dark web, leveraging their authorized access to bypass traditional security measures. On the other hand, an uninformed employee could inadvertently download malware by clicking on a phishing link, unknowingly creating a backdoor for external attackers. According to Silas and Rajsingh (2024), insider threats often exploit improper access controls, where users retain access to systems beyond what is necessary for their role, increasing the risk of unauthorized data exposure. Without stringent security protocols, organizations' trust in their employees can become a vulnerability.

The challenges in detecting and mitigating insider threats are compounded by the complexity of modern IT environments, where weak security settings, such as administrator accounts without strong passwords or active guest accounts, create fertile ground for exploitation. For example, an IT administrator might neglect to disable a former employee's account, leaving it vulnerable to unauthorized access long after the employee has left the organization. Additionally, the absence of network segmentation allows insiders unrestricted movement across systems once they gain initial access, enabling them to escalate privileges or access sensitive data unnoticed. The lack of real-time monitoring and auditing of user activities further exacerbates the problem, as suspicious behaviors—such as large data transfers during off-hours or repeated access attempts to restricted files—may go undetected until significant damage has occurred. Silas and Rajsingh (2024) emphasize that organizations must address these gaps through comprehensive security policies, continuous monitoring, and proactive auditing to promptly identify and respond to insider threats.

The complexities of managing insider threats also stem from the evolving nature of workplace dynamics, such as remote work arrangements and the widespread use of cloud-based applications, which increase the attack surface. For instance, an employee working remotely might connect to the corporate network using an unsecured personal device, inadvertently exposing sensitive data to cybercriminals through vulnerabilities in the device's software. Insider threats can also be facilitated by outdated security policies that fail to address new technological risks, such as the proliferation of shadow IT, where employees use unauthorized applications without the knowledge of the IT department. To mitigate these risks, organizations must enforce strict access controls based on the principle of least privilege, ensuring that employees only have access to the information necessary for their roles. Regular security audits, employee training programs, and the implementation of advanced threat detection tools that analyze user behavior for anomalies are critical components of a comprehensive insider threat management strategy (Silas & Rajsingh, 2024).

3.16 Malware Threats

Malicious code and malware threats pose a persistent and evolving challenge in the financial industry, exploiting technological vulnerabilities and human factors to infiltrate secure systems. Malware manifests in various forms, such as spyware that covertly monitors user activities, keystroke loggers that capture sensitive information like passwords and financial credentials, and Trojan horses disguised as legitimate software to gain unauthorized access. For instance, an employee at a financial institution might receive an email appearing to be from a trusted client containing an attachment labeled "quarterly financial report." Unbeknownst to the employee, opening the attachment activates a Trojan horse that silently installs spyware, allowing attackers to monitor transactions and exfiltrate confidential data. As Stanikzai et al. (2021) noted, malware often spreads through trusted data channels, making it difficult to detect because it blends seamlessly with routine business communications and processes. This deceptive nature complicates defense strategies, as traditional antivirus solutions may not identify newly engineered malware variants designed to evade detection.

The challenges in mitigating malware threats are compounded by attackers' sophisticated techniques, such as URL injections and fileless malware that operate entirely in a system's memory, leaving minimal traces for forensic analysis. Financial institutions face complexities not only in detecting these threats but also in managing the aftermath, as malware can disrupt operations, compromise customer data, and damage reputations. For example, a seemingly benign software update downloaded from a compromised third-party vendor could introduce adware that manipulates web traffic or redirects financial transactions to fraudulent sites without immediate detection. The reliance on automated processes in financial systems further exacerbates the risk, as malware can rapidly propagate across interconnected networks before security teams respond. Stanikzai et al. (2021) emphasize the importance of robust network security policies, such as implementing multi-layered defenses, regular system audits, and real-time monitoring tools to counteract these threats. Equally critical is employee education, ensuring that staff can recognize suspicious activities, avoid common phishing traps, and respond swiftly to potential breaches, strengthening the human firewall as an integral component of cybersecurity resilience.

3.17 Risk Threat Modeling

Threat modeling is a suitable defense mechanism to mitigate against risks faced by the organization. This is a process that analyzes potential design flaws in the system. According to the National Institute for Standards and Technology, "A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence" (National Institute of Standards and Technology, 2012). Threats and vulnerabilities evolve as technology, human behavior, and organizational policies change. Developing a risk threat matrix is necessary to visually comprehend the potential threats against the organization. Below is a tabular view of the

likelihood of a threat against the system versus the severity of the threat.

Table 1. Likelihood of a threat (left column) versus severity of a threat (top row)

Likelihood/Severity	Very Low – 1	Low – 2	Moderate – 3	High – 4	Very High – 5
Very High – 5	5	10	Vendor Risk - 15	Rootkits - 20	Worm/ransomware - 25
High – 4	4	8	12	DDoS- 16	Hacker Access/Phishing - 20
Moderate – 3	3	Physical damage - 6	9	Insider Threats - 12	15
Low – 2	2	4	Environmental damage - 6	8	10
Very Low – 1	1	2	3	4	5

3.18 Cloud Forensics

Due to the increase in cloud storage capabilities, numerous digital forensic investigations face the challenge of evidentiary artifacts stored on international soil. Unlike traditional digital forensics, cloud forensics presents a unique challenge due to the ubiquitous nature of the cloud. Typically, the corporate structure of cloud providers can be complex, leading to data jurisdiction concerns (Alshabibi et al., 2024).

According to (Alshabibi et al., 2024), **t**o ensure a secure and efficient recovery of data stored in the cloud:

1. Gathering information from cloud service providers.
2. Auditing activities that occurred within the cloud.
3. Obtaining evidence related to unauthorized access or any breaches.
4. Analyzing all the points to identify suspects.
5. Investigating and obtaining the outcome.

Cloud forensics primarily aims to ensure that digital evidence obtained from cloud-based services is authentic, credible, and admissible in court. By developing specialized techniques, instruments, and protocols for cloud-based investigations, professionals can detect evidence of online criminal activities, data breaches, and other unlawful actions involving cloud platforms (Alshabibi et al., 2024).

3.19 Regulatory Risks: Business Continuity and Incident Response

Financial institutions face regulatory risks associated with non-compliance with these data protection regulations, which can result in significant financial penalties and reputational damage (Bakare et al., 2024). Therefore, the financial industry must strategically prioritize compliance and data governance, leveraging technology and best practices to safeguard personal data and comply with various regulatory frameworks, ultimately maintaining operational viability internationally and domestically. It is essential to protect confidential information and systems in the face of a cyber-attack (Stanikzai et al., 2021). The more prepared a business is to respond to a potential cyber-attack, the faster the threat can be eradicated and reduce any damage to the business.

The speed and effectiveness of an institution's recovery plan significantly impact the severity of a cyber-attack. This incident response plan aims to quickly and effectively contain cyber-attacks and breaches (Kost, 2025). The actions outlined in the plan protect privileged accounts that provide access to critical systems such as databases, applications, and networks. A business continuity plan allows business to continue during and after an incident to critical infrastructure (Kost, 2025). The plan ensures that appropriate security controls are implemented and integrated into the system development (Deutsche Bank, 2025).

3.19.1 Enhancing Human Factors in Cybersecurity

To improve human factors in cybersecurity, financial institutions should implement continuous education and awareness programs that focus on social engineering threats, such as phishing and denial-of-service attacks. These programs should ensure that employees recognize and respond effectively to suspicious activities.

3.19.2 Optimizing Cybersecurity Process Improvement

For continuous process improvement in cybersecurity, institutions should adopt agile frameworks that allow for iterative testing, feedback loops, and incorporating lessons learned from security incidents into operational practices.

3.19.3 Advancing Cybersecurity Policies

Cybersecurity policies should be designed to align with international regulations and industry best practices. They should incorporate clear guidelines for incident response, data protection, and access control while maintaining flexibility to adapt to evolving threats.

3.19.4 Promoting Regulatory Compliance and International Cooperation

Given the fragmented nature of global cybersecurity regulations, financial institutions should advocate for greater international cooperation and harmonization of standards to ensure consistent protection across borders.

3.19.5 Integrating Business Continuity and Disaster Recovery Plans

Embedding robust business continuity and disaster recovery plans into cybersecurity strategies helps ensure operational resilience, with clear protocols for maintaining critical functions during and after cyber incidents.

3.19.6 Leveraging Advanced Technologies for Threat Mitigation

Adopting advanced technologies such as intrusion detection and prevention systems and secure cloud computing infrastructures can enhance the ability to detect, prevent, and respond to cyber threats in real-time.

3.19.7 Fostering a Culture of Cybersecurity Leadership

Leadership commitment to cybersecurity, demonstrated through resource allocation, executive training, and policy enforcement, fosters a culture of accountability and proactive risk management.

3.19.8 Conducting Regular Security Audits and Compliance Reviews

Institutions should conduct regular security audits, vulnerability assessments, and compliance reviews to identify gaps in security controls, assess the effectiveness of current policies, and ensure adherence to regulatory requirements.

4. Discussion

The financial sector remains a primary target for cybercriminals due to the high value of financial data and the increasing digitization of banking services. While regulatory frameworks such as the GDPR, Gramm-Leach-Bliley Act, and UK-GDPR establish guidelines for data protection, inconsistencies in state-level policies and rapid technological advancements create ongoing challenges for financial institutions. This study emphasizes the significance of proactive cybersecurity strategies, including business continuity planning, incident response mechanisms, and risk-based regulatory compliance. Emerging technologies such as cloud computing and artificial intelligence offer promising solutions for strengthening cybersecurity defenses but introduce new risks requiring careful management. Financial institutions must adopt a multi-layered approach to enhance cybersecurity resilience, balancing regulatory compliance with innovative security solutions.

4.1 Recommendations for Future Research

Future research should focus on international cooperation, evolving cyber threats, and integrating artificial intelligence in cybersecurity risk management to ensure a robust and adaptive financial security framework. To ensure protection against common cyber-attacks, security controls and countermeasures must be implemented within the critical infrastructure. In-depth implementation of defenses is vital for the financial industry to ensure the protection of assets. NIST 800-53 provides specific guidance on the application of security controls, including privacy controls and the process for selecting controls to protect a diverse set of threats. Additional recommendations include:

4.1.1 Collaboration

The current state of the financial market is well organized but lacks complete protections for individuals. While national policies provide adequate protections, state-level policies fail to regulate individual rights. Partnerships with other countries and collective nations demonstrate a growing need for an international body to determine the needs and rights of citizens and companies engaging in financial transactions.

4.1.2 Security Controls and Countermeasures

People are often the weakest link in the supply chain, leading to social engineering attacks (Nesterenko, 2024).

Financial institutions should consider more preventative controls. They should implement mandatory employee continuous training and user awareness, as well as multi-factor authentication, inventory of authorized software, limitations to network ports, vulnerability scanning, and penetration scanning.

4.1.3 Cloud computing

Cloud computing represents a recent innovation in the financial sector, offering numerous advantages such as simplified system backup and cost reduction for institutions (Cloud Technology Partners, n.d.). Financial institutions can optimize their profitability and allocate more resources to customer service and training by reducing the number of servers and associated heating and cooling costs.

4.1.4 Cybersecurity as a Service (CaaS):

As technology advances, cybersecurity measures are becoming more essential for financial institutions. Attackers are using more sophisticated methods. Smaller financial institutions should consider outsourcing cybersecurity services if a fully staffed security team is not readily available

4.1.5 Artificial Intelligence

From a regulatory standpoint, AI can potentially combat money laundering, financial terrorism, regulatory reporting, and additional solutions for fraud detection, customer service, etc. (Crisanto et al., 2024).

References

Alshabibi, M. M., Bu Dookhi, A. K., & Hafizur Rahman, M. M. (2024). Forensic investigation, challenges, and issues of cloud data: A systematic literature review. *Computers, 13*(8), 213. https://doi.org/10.3390/computers13080213

Bakare, S. S., Adeniyi, A. O., Akpuokwe, C. U., & Eneh, N. E. (2024). Data privacy laws and compliance: A comparative review of the EU GDPR and USA regulations. *Computer Science & IT Research Journal, 5*(3), 528–543. https://doi.org/10.51594/csitrj.v5i3.859

Bank of England. (2021). *CBEST: Intelligence-led testing for financial sector firms*. https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide.pdf

Bank of England. (2023). *Prudential regulation authority annual report 2023/24*. https://www.bankofengland.co.uk/prudential-regulation/publication/2024/july/pra-annual-report-2023-24

Bischoff, P. (2023, January 9). Internet privacy laws by state: Which US states best protect privacy online? *Comparitech*. https://www.comparitech.com/blog/vpn-privacy/which-us-states-best-protect-online-privacy/

Benaroch, M. (2018). Real options models for proactive uncertainty-reducing mitigations and applications in cybersecurity investment decision making. *Information Systems Research, 29*(2), 315–340. https://doi.org/10.1287/isre.2017.0714

Bernard, L., Raina, S., Taylor, B., & Kaza, S. (2021). Minimizing cognitive overload in cybersecurity learning materials: An experimental study using eye-tracking. In L. Drevin, N. Miloslavskaya, W. S. Leung, & S. von Solms (Eds.), *Information security education for cyber resilience* (pp. 47–63). Springer International Publishing. https://doi.org/10.1007/978-3-030-80865-5_4

Cloud Technology Partners. (n.d.). *Cloud adoption in the financial services industry*. Retrieved from https://www.cloudtp.com/doppler/cloud-adoption-financial-services-industry/

Crisanto, J. C., Leuterio, C. B., Prenio, J., & Yong, J. (2024). *Regulating AI in the financial sector: Recent developments and main challenges* (FSI Insights on Policy Implementation No. 63). Bank for International Settlements. https://www.bis.org/fsi/publ/insights63.pdf

De Groot, J. (2024, October 4). What is SOX compliance? What you need to know. *Digital Guardian*. https://digitalguardian.com/blog/what-sox-compliance

Darem, A. A., Alhashmi, A. A., Alkhaldi, T. M., Alashjaee, A. M., Alanazi, S. M., & Ebad, S. A. (2023). Cyber threats classifications and countermeasures in banking and financial sector. *IEEE Access, 11*, 125138–125158.

Deutsche Bank. (2025). *Business continuity program*. https://www.db.com/company/en/business-continuity-program.htm

Ebert, N., Schaltegger, T., Ambuehl, B., Schöni, L., Zimmermann, V., & Knieps, M. (2023). Learning from safety science: A way forward for studying cybersecurity incidents in organizations. *Computers & Security, 103*, 103435. https://doi.org/10.1016/j.cose.2023.103435

Fagade, T., Maraslis, K., & Tryfonas, T. (2017). Towards effective cybersecurity resource allocation: The Monte Carlo predictive modelling approach. *International Journal of Critical Infrastructures, 13*(2–3), 152–167. https://doi.org/10.1504/IJCIS.2017.088235

Federal Reserve Bank of New York. (2025). Cyber risk and the U.S. financial system: A pre-mortem analysis. *Economic Policy Review*. Retrieved from https://www.newyorkfed.org/medialibrary/media/research/epr/2025/EPR_2025_cyber-vulnerability_eisenbach.pdf

Federal Trade Commission. (n.d.). *Gramm-Leach-Bliley Act*. https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act

Financial Conduct Authority. (2024). *Regulating the financial sector: Cybersecurity and compliance*. Retrieved from https://www.fca.org.uk

First Bank & Trust Company. (2025, January 1). *Cybersecurity in 2025: What financial institutions need to know*. https://www.firstbank.com/resources/learning-center/cybersecurity-in-2025-what-financial-institutions-need-to-know/

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

Hasan, M., et al. (2022). *Qualitative research methods*. Tahta Media Group.

Information Commissioner's Office. (2023). *Guide to the General Data Protection Regulation (GDPR)*. https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf

Kennedy, E., & Joseph, O. (2024). A review of the impact of intrusion, detection and protection systems (IDPS) in cloud computing environment. *International Journal of Modelling & Applied Science Research, 6*(9), 215–222. https://cambridgeresearchpub.com/ijmasr/article/view/420/415

Kuner, C., Bygrave, L. A., & Docksey, C. (2020). *The EU General Data Protection Regulation (GDPR): A commentary*. Oxford University Press. https://doi.org/10.1093/oso/9780198826491.001.0001

Malatji, M., Von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information & Computer Security, 27*(2), 233–272. https://doi.org/10.1108/ICS-03-2018-0031

Malatji, M., Marnewick, A., & von Solms, S. (2020). Validation of a socio-technical management process for optimising cybersecurity practices. *Computers & Security, 95*, 101846. https://doi.org/10.1016/j.cose.2020.101846

Nesterenko, A. (2024, December 22). Banking cybersecurity challenges: Safeguarding financial institutions in 2025. *Dashdevs*. https://dashdevs.com/blog/cybersecurity-in-banking-main-threats-and-challenges-in-2023/

Ponemon Institute & IBM. (2024). *Cost of a data breach report 2024*. IBM. https://www.ibm.com/security/data-breach-report

Verizon. (2024). *2024 Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/dbir/

World Economic Forum. (2025). *Global cybersecurity outlook 2025*. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf