Advances in Machine Learning, IoT and Data Security

"Volume 1, Issue 2, Year 2025"

website: https://www.c5k.com

Research Article

Cyber Risk Analytics and Security Frameworks for Safeguarding U.S. Digital Banking Infrastructure

Md Fakhrul Hasan Bhuiyan[1*], Arafat Islam[2], AFM Rafid Hassan Akand[3], Ali Hassan[4], Sweety Rani Dhar[4], Durga Shahi[3], Adib Hossain[2], Arif Hosen[2]

[1]*Department of Information Studies, Trine University, Indiana, USA;*

[2]*Department of Business Analytics, Trine University, Indiana, USA;*

[3]*Department of Business Administration, Westcliff University, 400 Irvine, CA 92614, USA;*

[4]*Department of Business Administration, International American University, Los Angeles, CA 90010, USA;*

**Corresponding Author:* fakhrulbcef@gmail.com

ARTICLE INFO

Article history:
12 Sep 2025 (Received)
03 Oct 2025 (Accepted)
25 Oct 2025 (Published Online)

Keywords:
Cybersecurity, Banking Sector, Information Security, Regulatory Compliance, Artificial Intelligence, Risk Management.

ABSTRACT

This study explores the current landscape of information security policies and practices within the U.S. banking sector, while offering comparative insights from global banking systems. Using a qualitative approach and guided by PRISMA 2020 standards, the research involved a systematic review of 125 academic papers and 20 reports sourced from databases such as Scopus, Web of Science, and Google Scholar. The analysis reveals that U.S. banks face a wide array of cybersecurity threats, including phishing, ransomware, insider risks, and regulatory challenges. Nevertheless, robust security frameworks anchored by legislation like the Gramm-Leach-Bliley Act and supported by partnerships with agencies such as CISA and FS-ISAC—have helped mitigate these risks by fostering trust, enhancing fraud detection through AI, and maintaining financial stability. Global comparisons highlight shared concerns over evolving threats, regulatory compliance, and the importance of international collaboration. While the U.S. demonstrates strong regulatory foundations, areas for improvement include enhanced employee training, broader adoption of advanced cybersecurity tools, and greater cross-border coordination. The study concludes by recommending multi-factor authentication, AI and blockchain integration, and increased employee awareness initiatives. However, it notes limitations such as the reliance on secondary data and a U.S.-centric focus. Future research should include primary data and quantitative evaluations to better understand the effectiveness of cybersecurity investments. These findings offer practical guidance for policymakers and banking stakeholders aiming to strengthen cyber resilience in an increasingly digital financial environment.

DOI: https://doi.org/10.63471/amlids_25002

1. Introduction

In today's highly digitized financial environment, information security has become a foundational element in ensuring the stability, integrity, and trustworthiness of global banking systems. The banking sector, more than most industries, faces an ever-growing wave of cyber threats due to the vast amounts of sensitive financial and personal data it processes daily. In the United States, home to one of the most interconnected and digitized financial systems, robust information security frameworks are both a legal obligation and a vital mechanism to maintain public confidence and economic resilience (Abrahams et al., 2024).

Recent years have witnessed a dramatic escalation in cyberattacks targeting financial institutions, with tactics ranging from ransomware and phishing to insider threats and denial-of-service attacks. According to Hassan et al. (2024), breaches not only disrupt operations but also carry long-term reputational damage, financial loss, and erosion of stakeholder trust. A notable case involved a major New York bank where

*Corresponding author: fakhrulbcef@gmail.com (Md Fakhrul Hasan Bhuiyan)

Cite: Md Fakhrul Hasan Bhuiyan, Arafat Islam, AFM Rafid Hassan Akand, Ali Hassan, Sweety Rani Dhar, Durga Shahi, Adib Hossain, Arif Hosen (2025). Cyber Risk Analytics and Security Frameworks for Safeguarding U.S. Digital Banking Infrastructure. *Advances in Machine Learning, IoT and Data Security,* 1(2), pp. 1-11.

cybercriminals gained access to customer data, including names, addresses, and contact information. While no financial fraud was detected, the incident underlines the sophistication of contemporary attackers and the evolving nature of cyber threats in the sector (Teng et al., 2023).

In this context, information security has expanded beyond IT departments and has become a boardroom-level concern. The growing reliance on digital platforms has exposed systemic vulnerabilities in legacy systems and outdated protocols. As cybercriminals exploit these gaps, financial institutions are being pushed to adopt proactive, rather than reactive, approaches. Moreover, Alawida et al. (2023) emphasize that cyber threats have moved from isolated events to persistent, state-sponsored campaigns targeting national infrastructure, particularly in economically strategic nations like the U.S. The regulatory landscape in the United States has evolved significantly to address these threats. Laws such as the Gramm-Leach-Bliley Act, along with initiatives like the Cybersecurity and Infrastructure Security Agency (CISA) and the Financial Services Information Sharing and Analysis Center (FS-ISAC), aim to bolster institutional defenses and encourage industry-wide cooperation. However, these regulations often struggle to keep pace with the speed of technological advancement and the growing interconnectivity of global finance (Challoumis & Eriotis, 2024). Furthermore, there is a critical need for regulatory synchronization across borders to ensure that cross-national data transfers and banking activities remain secure under varied legal frameworks (Rahman et al., 2024). Human error and behavioral factors remain among the leading causes of data breaches. According to Bhuiyan (2024), employees often unknowingly act as the weakest link in the information security chain. Despite technological safeguards, incidents of phishing, unauthorized access, and credential leaks are often the result of poor training or policy non-compliance. Allioui and Mourdi (2023) point out that organizational culture, continuous education, and internal audits are essential components of a resilient information security environment.

In addition, modern banking increasingly relies on third-party vendors, shared platforms, and cloud-based systems. These interdependencies introduce new layers of risk. Ahmed and Khan (2023) stress that without strict vendor management policies and real-time monitoring, financial institutions risk losing visibility and control over their data, creating opportunities for external exploitation. Customers, too, are more concerned than ever about how their personal data is stored, used, and protected. Studies by Prastyanti and Sharma (2024) show that concerns about privacy and identity theft have led to rising demand for transparency and accountability in data governance practices.

Technologically, banks are beginning to adopt advanced solutions such as AI**,** ML**,** and blockchain to enhance threat detection, automate risk management, and protect against fraudulent transactions. AI-based systems are particularly effective at analyzing large volumes of data in real time, detecting unusual patterns, and responding faster than manual systems (Uddin et al., 2020). However, reliance on automated tools must be balanced with strategic oversight, as overdependence on technology can create blind spots, especially if algorithms are poorly trained or biased.

Social engineering remains one of the most effective strategies used by cybercriminals. Phishing attacks—where users are tricked into revealing credentials or clicking malicious links—continue to rise. Attackers often combine technical exploits with psychological manipulation, targeting both customers and employees (Mahmud et al., 2024). Furthermore, malware such as spyware and trojans are deployed to gather login details and transaction histories without immediate detection. According to Hossain et al. (2024) , the rapid digitization of financial services has not only opened doors to innovation but also made systems more vulnerable to complex attack vectors. Despite the evident risks, empirical research on cybersecurity governance in the U.S. banking sector remains relatively underdeveloped. As noted by Kshetri et al. (2023), much of the current framework is built upon anecdotal evidence and case studies rather than rigorous, evidence-based strategies. This lack of standardized practices hinders comprehensive risk assessment and policy formulation. As summarized in Table 1, the literature reveals clear research gaps, particularly in areas concerning long-term effectiveness of security investments, cross-sector collaboration, and employee engagement strategies.

Table 1. A list of papers for addressing the research gaps

Source	Purposes	Methodology	Implications
Hassan et al. (2024)	To examine cybersecurity practices in the global banking sector with a focus on Nigerian banks.	Qualitative, literature review	Provides insights into regional cybersecurity frameworks and the need for stronger compliance measures.
Prastyanti and Sharma (2024)	To analyze the role of data protection law in establishing consumer trust in banking.	Quantitative survey	Highlights the role of regulatory frameworks in enhancing data security and consumer confidence.

Hossain et al. (2024)	To explore the effectiveness of AI and machine learning in fraud detection within the banking sector.	Case study, qualitative	Provides practical insights into the integration of AI in banking security to prevent fraud.
Mabaso and Booi (2024)	To assess the balance between privacy and national security in U.S. information security policies.	Qualitative, policy analysis	Emphasizes the need for a balanced approach to privacy and security, particularly in the banking sector.
Guseva (2024)	To evaluate the role of decentralized markets and regulations in shaping banking information security.	Qualitative, conceptual analysis	Suggests the future role of decentralized finance (DeFi) in reducing cybersecurity risks in traditional banking.
Pereira and Viola (2024)	To examine the evolution of U.S. banking regulation and its response to emerging cybersecurity risks.	Historical analysis, qualitative	Highlights the changing regulatory frameworks and their impact on cybersecurity resilience in banking.
Adeniran et al. (2024)	To evaluate risk management strategies in U.S. financial institutions concerning regulatory compliance.	Mixed-methods, case studies	Provides strategies for U.S. banks to enhance their cybersecurity frameworks while ensuring regulatory compliance.
Faraji et al. (2024)	To explore the role of artificial intelligence in preventing financial fraud in U.S. banks.	Empirical research, AI application	Demonstrates how AI can significantly reduce fraud risks by improving detection and response systems.
Kaur et al. (2023)	To investigate the potential of AI for enhancing cybersecurity measures in banking institutions.	Literature review, AI-focused	Suggests AI-based solutions for real-time threat detection and response systems in financial institutions.
Jaiwani and Gopalkrishnan (2024)	To explore how private asset reconstruction companies influence financial stability.	Case study, qualitative	Highlights the role of private asset management in ensuring the financial stability and cybersecurity of banking systems.

Given these challenges, this study sets out two core objectives. First, it seeks to examine the existing information security policies and practices in the U.S. banking sector, focusing on identifying associated risks, operational benefits, and broader impacts on financial stability. Second, it aims to evaluate how the U.S. framework compares to global banking systems, offering insights into emerging trends and proposing strategies for improved international cooperation and regulatory alignment.

2. Literature Review

2.1. Information Security & Policy

Information security, an essential subset of information risk management, focuses on minimizing the likelihood of unauthorized access and misuse of sensitive data. It includes preventing data breaches, corruption, deletion, unauthorized disclosure, and other forms of cyber threats[22]. In modern banking institutions, especially in the United States, information security policies serve as the foundation for ensuring confidentiality, integrity, and availability of financial data. These policies encompass standards, protocols, and procedures developed to protect IT systems. The effectiveness of an organization's entire privacy strategy often hinges on the robustness of its information security policy. Faraji, et al. [19] emphasize that a carefully designed and enforced policy forms the backbone of any secure infrastructure. AL-Hawamleh [23] further argues that establishing a formal information security policy is a critical first step in defending against both internal and external threats. This assertion aligns with the structured policy development models proposed by Mimi, et al. [24], which institutions can use to regularly evaluate and enhance their security frameworks. Figure 1 illustrates the layered structure of a comprehensive information security policy within a banking framework.

Figure 1. US Information and Infrastructure Security Agency [25]

2.2. The United States Information Security Scenario

In a time when digital transformation drives economic growth and reshapes national security frameworks, the U.S. government has increasingly prioritized cybersecurity, particularly within critical sectors like banking. The Biden administration has taken active steps to address the vulnerabilities associated with a globally connected financial system. A major challenge for U.S. banking lies in maintaining a delicate balance between data privacy and national security. As noted by Mabaso and Booi [15], the current regulatory environment reflects this tension, where safeguarding citizens' private information sometimes limits the government's surveillance capabilities, even in contexts of national defense [26].

Additionally, the rapid globalization of banking has blurred the distinctions between domestic and foreign financial institutions, with international banks gaining competitive ground in U.S. markets. The growing presence of foreign banks has led to increased political and regulatory scrutiny. Mimi, et al. [24] suggest that current shifts in the financial landscape including a reduced reliance on banks for external funding and an increase in non-interest-generating activitiesnecessitate regulatory reform. Moreover, systemic risks have prompted regulators to adopt a macroprudential approach, prioritizing the stability of the financial system as a whole rather than focusing solely on individual institutions. These evolving dynamics are reflected in Table 2, which summarizes the major policy and structural adjustments within the U.S. banking cybersecurity landscape.

Table 2. Key points about information security in worldwide banking

Key points	Description	Reference
Evolving Threat Landscape	The landscape poses significant authority to enforce consumer protection laws, while digital transformation and technologies like AI and blockchain expand cyber-attack surfaces.	Kamar, et al. [27]
Regulatory Compliance	Banks must follow local and international standards to manage risks from data breaches and cyberattacks, enhancing customer trust.	Adeniran, et al. [18]
Data Privacy and Protection	Banks employ encryption and regulatory frameworks (e.g., GDPR, CCPA) to protect sensitive customer data from breaches and cyber threats.	Wang, et al. [28]
International Cooperation	Cross-border collaboration strengthens threat intelligence sharing, global security standards, and coordinated responses to cyber incidents.	Hassan, et al. [2]

2.3. Importance of Studying the U.S. Banking Systems

With the digitalization of financial transactions and widespread storage of sensitive data, cybersecurity has become a central concern for financial institutions worldwide. Studying the U.S. banking system is particularly relevant given its scale, influence, and integration into the global economy. Saeed, et al. [29] It is essential to highlight that understanding country-specific cybersecurity strategies is crucial for developing effective countermeasures against evolving threats. One area of growing concern is the fight against money laundering, which poses serious economic and reputational risks. According to Akartuna, et al. [30], robust information security measures are essential to detect, prevent, and respond to such illicit activities.

Furthermore, analyzing the U.S. banking sector provides insights into how cybersecurity frameworks and global standards are interpreted and implemented in practice. Khan, et al. [31] argue that adapting security protocols to match the specific requirements of financial institutions is crucial for sustainable operations. Given the increasing interdependence of banking systems across borders, identifying cybersecurity risks and their economic implications helps regulators and industry stakeholders strengthen defenses. Uddin, et al. [11] emphasize that the growing interconnectivity of banks has made the sector more vulnerable to coordinated attacks, thus reinforcing the urgency of comprehensive

cybersecurity planning. The importance of such analysis is also supported by Dwivedi, et al. [32], who note that understanding these vulnerabilities is key to shaping responsive and adaptive cybersecurity policy.

2.4. U.S. Banking Information Security Risks and Rewards

The U.S. banking sector faces a constantly shifting threat landscape shaped by rapid technological progress and increasingly sophisticated cyberattacks. Alam and Afrin [33] describe an environment where risks such as phishing scams, ransomware, and insider threats are ever-present. With banks storing vast quantities of financial and personal data, they have become primary targets for cybercriminals seeking financial gain or intent on disrupting national infrastructure. Ransomware, in particular, has emerged as a major threat, capable of paralyzing banking operations and causing significant reputational and economic losses. Phishing attacks—often directed at employees and clients—exploit human error to compromise internal systems. Additionally, noncompliance with federal regulations like the Gramm-Leach-Bliley Act or Payment Card Industry Data Security Standard (PCI DSS) can result in substantial legal and financial penalties. Despite these challenges, there are substantial rewards for institutions that invest in advanced information security programs. Strengthening cybersecurity frameworks builds customer trust—an invaluable asset in today's competitive market. Technologies such as AI and machine learning play a pivotal role in enhancing fraud detection and incident response capabilities. AL-Hawamleh [23] highlights those automated systems reduce human error and improve operational resilience. Additionally, well-secured financial institutions tend to attract more investors and maintain long-term market credibility.

Strategic partnerships with government agencies and global coalitions further enhance cybersecurity readiness. Programs like CISA and FS-ISAC enable intelligence sharing, incident coordination, and policy alignment across the sector [34]. These collaborations reflect a proactive stance, reinforcing the role of U.S. banks as leaders in financial data protection. As visualized in Figure 1, the integration of security strategies, regulatory compliance, and emerging technologies contributes to a layered defense system. By striking a balance between innovation and risk mitigation, U.S. financial institutions can remain agile in the face of emerging threats while maintaining robust, secure operations in an increasingly digital economy.

3. Methodology

3.1 Research Design and Objectives

This study adopts a qualitative research approach, drawing primarily on secondary data to examine the state of information security within the U.S. banking sector. The research aims to explore existing policies and practices, with a focus on identifying key risks, benefits, and their broader implications for financial systems [35]. In addition, the study compares the U.S. information security framework with those of global banking institutions to uncover shared trends, systemic challenges, and strategic opportunities for strengthening cybersecurity on an international scale. The methodology is guided by a structured research design that enables in-depth analysis of complex information environments through well-established qualitative techniques.

3.2 Data Sources and Search Strategy

Data for this research were sourced from a wide range of reputable secondary sources, including peer-reviewed journals, academic publications, media reports, and credible online platforms. The literature search was conducted using leading academic databases such as Science Direct**,** Scopus**,** Web of Science**,** PubMed**,** DOAJ, and Google Scholar**.** To ensure consistency and academic rigor, the data collection process followed the PRISMA 2020 (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines. Although originally developed for clinical and randomized trial studies, PRISMA's framework has been effectively adapted for systematic reviews in broader disciplines, including those related to finance and cybersecurity [36]. This standardized protocol enhances transparency and replicability in reporting qualitative reviews.

3.3 Inclusion and Exclusion Criteria

The review process incorporated targeted keyword searches aligned with the study's goals. Search terms included phrases such as "comparison to global banking systems," "identifying significant trends," "cybersecurity challenges," and "information security enhancement." Publications were evaluated based on relevance to the study's scope. Articles that failed to match the keyword criteria or diverged from the subject focus were removed during the screening stage. Furthermore, exclusion criteria were applied to eliminate studies with insufficient data, non-English language publications, inconsistent findings, or fragmented data presentation. This rigorous vetting process ensured that only high-quality and relevant literature was retained.

3.4 Data Selection Outcome

Following multiple stages of screening and refinement, a total of 125 scholarly articles and 20 official reports were selected for detailed review and analysis. These documents form the empirical basis of the study and contribute to a comprehensive understanding of the information security environment in the U.S. banking sector. The literature selection process and filtering results are visually summarized in Figure 2, which presents the PRISMA-based flow diagram of study identification, screening, eligibility, and inclusion. This

figure supports methodological transparency and confirms adherence to established systematic review standards.

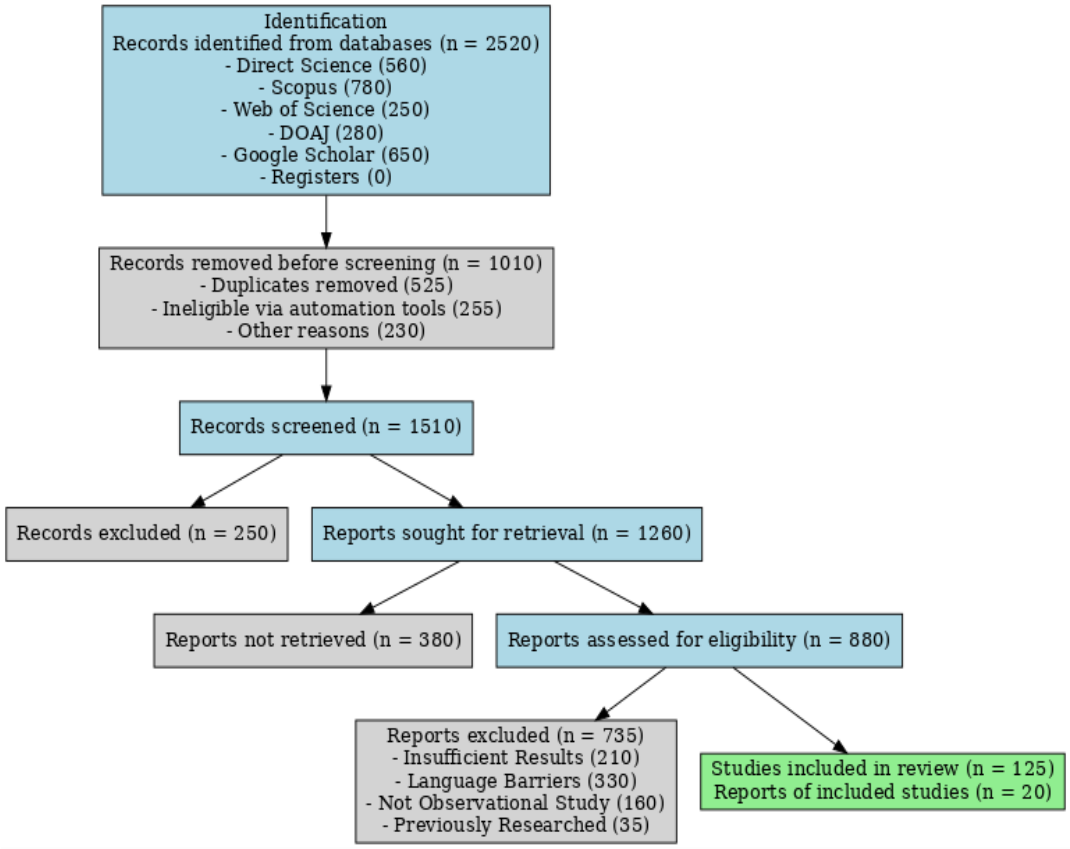

Figure 2. Systematic review methodology

4. Discussion

4.1. U.S. Banking and Financial Landscape

The U.S. banking system operates within a dynamic financial environment shaped by fierce competition, risk management practices, the role of financial intermediaries, and the transmission of monetary policy. Coker, et al. [37] emphasize the significance of these elements in maintaining economic equilibrium. The system is supported by mechanisms such as deposit insurance and liquidity provisions that play a vital role in averting bank runs and ensuring market stability. As regulatory measures evolve to maintain system integrity, Alam, et al. [38] argue that understanding the impact of financial expansion on risk-taking is crucial. While the expansion of credit access brings benefits, it also amplifies exposure to systemic vulnerabilities, particularly within the U.S. banking sector. These factors reinforce the importance of policy oversight and risk-mitigation strategies. *Table 3* summarizes key attributes of the U.S. banking ecosystem, illustrating the interplay between financial development and risk concentration.

4.2. Information Security in Worldwide Banking

The globalization of banking, accelerated by regulatory shifts like the International Banking Act of 1978, brought U.S.-based foreign bank branches under federal supervision, marking a pivotal shift from previously fragmented state-level control. Across international banking systems, Information Security Awareness (ISA) is increasingly acknowledged as a core element in fostering secure institutional behavior. ISA reflects a state in which employees are well-informed and committed to organizational cybersecurity objectives [39].

As these awareness levels can diminish over time, continuous renewal and reinforcement through policies and training are essential—particularly in the banking industry where the stakes are high. Mabaso and Booi [15] document how both traditional (e.g., printed materials, instructor-led sessions) and digital tools (e.g., intranet portals, online training modules) are used to refresh and disseminate cybersecurity practices. A case study involving a global bank showed that awareness was sustained through workshops, visual communication, and digital learning initiatives aligned with internal ISPs. *Figure 3* provides a conceptual overview of communication channels used in ISA

programs across global banks. Additionally, contemporary issues such as data protection, regulatory compliance, international collaboration, and evolving cyber threats remain central to global banking security.

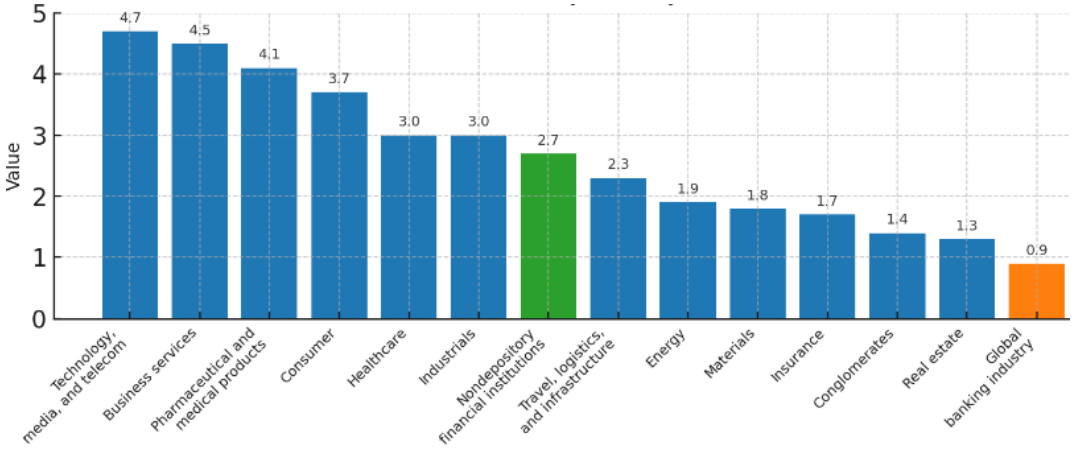

Figure 3. Price-to-Book ratio, by industry, 2023 [25]

4.3. Recommendations for Strengthening Cybersecurity in Banking

Given the increasing complexity and frequency of cyber threats targeting financial institutions, especially within the U.S., this study outlines several key recommendations for enhancing cybersecurity resilience. First, financial entities must adopt proactive cybersecurity strategies including multi-factor authentication, resilient digital infrastructure, and periodic security audits to detect and prevent vulnerabilities before exploitation occurs.

Second, employee training remains a cornerstone of defense, as human error often serves as a gateway for breaches. Continuous awareness campaigns and skill development programs can empower staff to respond effectively to emerging threats. Third, adopting recognized cybersecurity frameworks, such as NIST or ISO/IEC 27001, enables institutions to manage risks in a structured and adaptable way [20].

Lastly, embracing technological innovation, including artificial intelligence for threat detection, machine learning for fraud analytics, and blockchain for transaction integrity, can significantly enhance cybersecurity capabilities. These strategies, detailed in *Table 3*, serve as actionable guidelines for banks aiming to build future-ready cyber defense systems.

Table 3. Oversight and supervision of support for cybersecurity

Item	Description	Reference
Systemic Risk Identification and Support (SyRIS)	Assesses and mitigates risks with intra/interagency collaboration, offering expertise across risk domains to support OCC supervision.	Conti-Brown and Feinstein [40]
Bank Supervision Policy (BSP)	Includes divisions for cybersecurity policy, critical infrastructure, and operational risk to guide examination and manage systemic risks.	Prastyanti and Sharma [10]
The Office of Financial Technology	Acts as the OCC's central unit for banking innovation, coordinating cybersecurity and operational resilience for emerging technologies.	Saeed, et al. [29]

4.4. Implementation of Cybersecurity Policies and Procedures

Effective cybersecurity in banking requires not only strategy but also strong governance and implementation oversight. As noted by George, et al. [41], U.S. bank supervisors, particularly the Office of the Comptroller of the Currency (OCC), emphasize operational resilience through clearly defined risk management policies, incident response mechanisms, and continuity plans. The OCC's 2024 supervision plan prioritizes cyber risk management across national banks, federal savings associations, and third-party vendors. Compared to other global banking systems, the U.S. stands out for its regulatory sophistication but also contends with unique challenges arising from fast-paced

technological developments and an increasingly complex threat landscape.

Key global trends such as heightened attention to data privacy, integration of blockchain, and the demand for cross-border collaboration are reshaping how financial institutions approach cybersecurity. While U.S. banks possess advanced infrastructure and strong legal frameworks, this study identifies critical areas for enhancement. Strengthening proactive security measures, including multi-factor authentication and continuous training, remains essential. Additionally, banks must leverage advanced technologies and adopt adaptable cybersecurity frameworks to remain resilient against evolving threats. These insights affirm the need for cybersecurity strategies that are both globally informed and locally applicable, ensuring that U.S. institutions remain secure and competitive in a digital-first financial environment.

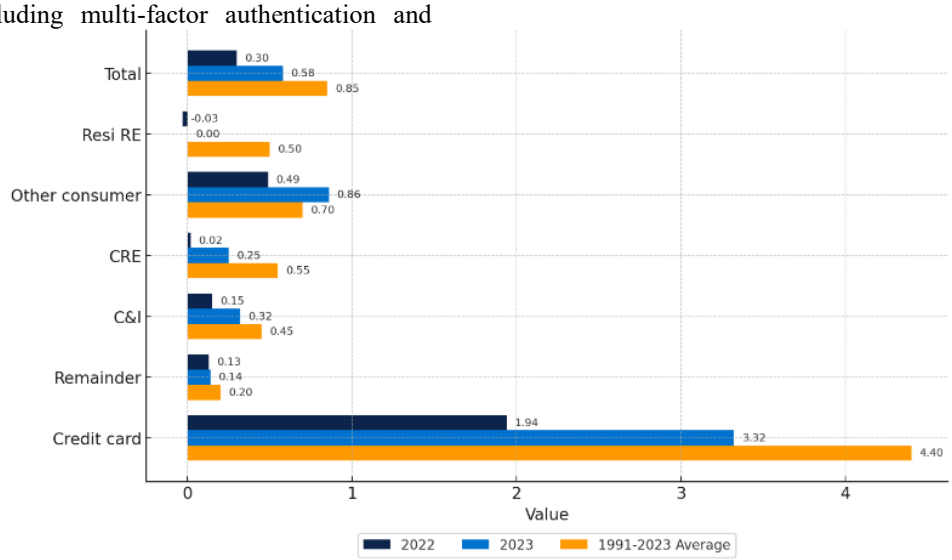

Figure 4. Net charge-off rates for the federal banking system

5. Conclusions

This study presents an in-depth exploration of the information security landscape in the U.S. banking sector, shedding light on current practices, associated risks, and strategic responses. By employing a qualitative research framework supported by a systematic review of secondary sources, the research identifies key trends and challenges in cybersecurity within the financial domain. A central finding of this analysis is the high level of vulnerability that U.S. banks face in the face of modern cyber threats, including phishing schemes, ransomware attacks, and insider breaches. These risks, though significant, are counterbalanced by the considerable benefits that robust cybersecurity strategies can offer. Financial institutions that adopt cutting-edge technologies such as artificial intelligence and machine learning are better positioned to detect threats early, enhance operational resilience, and foster greater trust among their customer base.

The study also underscores the essential role of regulatory compliance in maintaining the integrity of financial systems. U.S. banks that align their operations with legislative frameworks such as the Gramm-Leach-Bliley Act and actively collaborate with organizations like the Cybersecurity and Infrastructure Security Agency (CISA) and the Financial Services Information Sharing and Analysis Center (FS-ISAC) are more equipped to withstand and respond to emerging cybersecurity challenges.

Beyond the operational insights, the study provides meaningful implications for policymakers and regulators. It highlights the urgency of adopting proactive risk management strategies, investing in ongoing employee training, and fostering international cooperation to create a unified front against cybercrime. These findings can guide strategic decision-making at both institutional and governmental levels, promoting stronger and more adaptive cybersecurity cultures.

However, the research is not without limitations. The exclusive reliance on secondary data restricts the ability to capture real-time developments and contextual insights that primary data might reveal. Future research should consider incorporating empirical studies, surveys, or case-based analyses to deepen the understanding of how cybersecurity investments influence financial and operational outcomes within banks.

Ultimately, the study concludes that the U.S. banking sector must remain agile and forward-thinking in its approach to information security. As the threat landscape evolves and technological innovations accelerate, banks must continue to refine their cybersecurity frameworks to safeguard assets, maintain public confidence, and ensure the sustained stability of the nation's financial infrastructure.

6. Limitations and Future Directions

This study is primarily based on secondary data sources, including academic publications, industry reports, and media coverage. While these resources offer valuable insights, they also present certain limitations—particularly in terms of capturing the most recent developments within the U.S. banking sector's information security landscape. As cyber threats continue to evolve rapidly, relying solely on existing literature may result in gaps, particularly concerning emerging risks and newly adopted security strategies. Moreover, the exclusive focus on the U.S. banking system means the findings may not fully apply to other countries, especially those operating under different regulatory frameworks and facing distinct cybersecurity challenges.

Another notable limitation lies in the qualitative nature of the research. While it provides an in-depth understanding of institutional policies and trends, it does not allow for empirical measurement of the effectiveness or outcomes of those frameworks. As such, the study lacks a statistical perspective that could help quantify the impact of cybersecurity practices across a wider range of financial institutions.

To build on this foundation, future research should incorporate primary data collection methods, such as surveys, interviews, or field studies involving cybersecurity professionals, IT administrators, and financial stakeholders. These approaches can capture real-time experiences and reveal practical challenges that may not be evident through secondary analysis alone. Additionally, quantitative studies could enhance the robustness of future investigations by measuring the cost-effectiveness, success rates, and performance metrics of various cybersecurity strategies employed by financial institutions.

Another promising direction is to explore cross-border data-sharing mechanisms and assess the effectiveness of international cooperation in addressing global cyber threats. Comparative studies across different jurisdictions could provide valuable insights into how diverse regulatory environments influence security outcomes. Moreover, as the banking sector increasingly adopts advanced technologies, future research should also examine the impact of innovations such as artificial intelligence, blockchain, and quantum computing in enhancing data protection, threat detection, and risk mitigation strategies.

Finally, deeper exploration into the human dimension of cybersecurity, particularly employee compliance, behavior, and awareness, could provide critical input for designing more effective training programs and cultivating a stronger security culture within banks. Understanding how human factors intersect with technical safeguards will be vital in developing comprehensive, resilient cybersecurity systems that can withstand both internal and external threats.

References

[1] T. O. Abrahams, S. K. Ewuga, S. O. Dawodu, A. O. Adegbite, and A. O. Hassan, "A review of cybersecurity strategies in modern organizations: Examining the evolution and effectiveness of cybersecurity measures for data protection," *Computer Science & IT Research Journal,* vol. 5, no. 1, pp. 1-25, 2024.

[2] A. O. Hassan, S. K. Ewuga, A. A. Abdul, T. O. Abrahams, M. Oladeinde, and S. O. Dawodu, "Cybersecurity in banking: a global perspective with a focus on Nigerian practices," *Computer Science & IT Research Journal,* vol. 5, no. 1, pp. 41-59, 2024.

[3] H.-W. Teng *et al.*, "Mitigating digital asset risks," 2023.

[4] M. Alawida, S. Mejri, A. Mehmood, B. Chikhaoui, and O. Isaac Abiodun, "A comprehensive study of ChatGPT: advancements, limitations, and ethical considerations in natural language processing and cybersecurity," *Information,* vol. 14, no. 8, p. 462, 2023.

[5] C. Challoumis and N. Eriotis, "A historical analysis of the banking system and its impact on Greek economy," *Edelweiss Applied Science and Technology,* vol. 8, no. 6, pp. 1598-1617, 2024.

[6] M. M. Rahman, M. R. I. Bhuiyan, and S. A. Alam, "The empirical study on the impact of the COVID-19 on small and medium enterprises (SMEs) in Bangladesh," *Journal of Information Systems and Informatics,* vol. 6, no. 1, pp. 527-547, 2024.

[7] M. R. I. Bhuiyan, "Examining the digital transformation and digital entrepreneurship: A PRISMA based systematic review," *Pakistan Journal of Life and Social Sciences,* vol. 22, no. 1, pp. 1136-1150, 2024.

[8] H. Allioui and Y. Mourdi, "Exploring the full potentials of IoT for better financial growth and stability: A comprehensive survey," *Sensors,* vol.

23, no. 19, p. 8015, 2023, doi: 10.3390/s23198015

[9] S. Ahmed and M. Khan, "Securing the Internet of Things (IoT): A comprehensive study on the intersection of cybersecurity, privacy, and connectivity in the IoT ecosystem," *AI, IoT and the Fourth Industrial Revolution Review,* vol. 13, no. 9, pp. 1-17, 2023.

[10] R. A. Prastyanti and R. Sharma, "Establishing Consumer Trust Through Data Protection Law as a Competitive Advantage in Indonesia and India," *Journal of Human Rights, Culture and Legal System,* vol. 4, no. 2, pp. 354-390, 2024.

[11] M. H. Uddin, M. H. Ali, and M. K. Hassan, "Cybersecurity hazards and financial system vulnerability: a synthesis of literature," *Risk Management,* vol. 22, no. 4, pp. 239-309, 2020.

[12] T. Mahmud, M. A. H. Prince, M. H. Ali, M. S. Hossain, and K. Andersson, "Enhancing Cybersecurity: Hybrid deep learning approaches to smishing attack detection," *Systems,* vol. 12, no. 11, p. 490, 2024.

[13] R. Hossain, A. Al-Amin, L. Mani, M. Islam, T. Poli, and M. Milon, "Exploring the Effectiveness of Social Media on Tourism Destination Marketing: An Empirical Study in a Developing Country," *Wseas Trans. Bus. Econ,* vol. 21, pp. 1392-1408, 2024.

[14] N. Kshetri *et al.*, "“So what if ChatGPT wrote it?” Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy," *International Journal of Information Management,* vol. 71, p. 102642, 2023.

[15] C. Mabaso and O. Booi, "Exploring the precarious employment practices and decent work objectives In South Africa: A comprehensive analysis," *Journal of Namibian Studies,* pp. 312-341, 2024.

[16] Y. Guseva, "Decentralized markets and self-regulation," *Geo. Wash. L. Rev.,* vol. 92, p. 1281, 2024.

[17] J. C. Pereira and E. Viola, "From protagonist to laggard, from pariah to phoenix: Emergence, decline, and re-emergence of Brazilian climate change policy, 2003–2023," *Latin American Policy,* vol. 15, no. 3, pp. 400-422, 2024.

[18] I. A. Adeniran, A. O. Abhulimen, A. N. Obiki-Osafiele, O. S. Osundare, E. E. Agu, and C. P. Efunniyi, "Strategic risk management in financial institutions: Ensuring robust regulatory compliance," *Finance & Accounting Research Journal,* vol. 6, no. 8, pp. 1582-1596, 2024.

[19] M. R. Faraji, F. Shikder, M. H. Hasan, M. M. Islam, and U. K. Akter, "Examining the role of artificial intelligence in cyber security (CS): A systematic review for preventing prospective solutions in financial transactions," *International Journal,* vol. 5, no. 10, pp. 4766-4782, 2024.

[20] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," *Information Fusion,* vol. 97, p. 101804, 2023/09/01/ 2023, doi: https://doi.org/10.1016/j.inffus.2023.101804.

[21] M. Jaiwani and S. Gopalkrishnan, "Global resurgence: private asset reconstruction companies as legal catalysts for financial stability in India and beyond," *International Journal of Law and Management,* 2024.

[22] M. T. Alshurideh, E. K. Alquqa, H. M. Alzoubi, B. Al Kurdi, and S. Hamadneh, "The effect of information security on e-supply chain in the UAE logistics and distribution industry," *Uncertain Supply Chain Management,* vol. 11, no. 1, pp. 145-152, 2023.

[23] A. AL-Hawamleh, "Cyber resilience framework: Strengthening defenses and enhancing continuity in business security," *International Journal of Computing and Digital Systems,* vol. 15, no. 1, pp. 1315-1331, 2024.

[24] A. Mimi, M. A. Imran, T. H. Beg, and M. S. Rahman, "Governmental and Institutional Initiatives And Actions For The Attraction And Expansion Of E-Commerce By Women In Bangladesh," *American Economic & Social Review,* vol. 9, no. 1, pp. 17-28, 2022.

[25] M. W. Ullah, M. T. Alam, T. Sultana, M. M. Rahman, M. R. Faraji, and M. F. Ahmed, "A systematic review on information security policies in the USA banking system and global banking: Risks, rewards, and future trends," *Edelweiss Applied Science and Technology,* vol. 8, no. 6, pp. 8437-8453, 2024.

[26] S. Gulyamov and S. Raimberdiyev, "Personal data protection as a tool to fight cyber corruption," *International Journal of Law and Policy,* vol. 1, no. 7, pp. 1-35, 2023.

[27] E. Kamar, C. J. Howell, D. Maimon, and T. Berenblum, "The moderating role of thoughtfully reflective decision-making on the relationship between information security messages and smishing victimization: An experiment," *Justice Quarterly,* vol. 40, no. 6, pp. 837-858, 2023.

[28] S. Wang, M. Asif, M. F. Shahzad, and M. Ashfaq, "Data privacy and cybersecurity challenges in the digital transformation of the banking sector," *Computers & security,* vol. 147, p. 104051, 2024.

[29] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, "Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations," *Sensors,* vol. 23, no. 15, p. 6666, 2023.

[30] E. A. Akartuna, S. D. Johnson, and A. Thornton, "Preventing the money laundering and terrorist financing risks of emerging technologies: An international policy Delphi study," *Technological Forecasting and Social Change,* vol. 179, p. 121632, 2022.

[31] H. H. Khan, S. Khan, and A. Ghafoor, "Fintech adoption, the regulatory environment and bank stability: An empirical investigation from GCC economies," *Borsa Istanbul Review,* vol. 23, no. 6, pp. 1263-1281, 2023.

[32] Y. K. Dwivedi *et al.*, "Opinion Paper:"So what if ChatGPT wrote it?" Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy," *International journal of information management,* vol. 71, p. 102642, 2023.

[33] S. Alam and S. Afrin, "A Conceptual Framework for Family Business Strategic Direction in the Bangladeshi Readymade Garment Industry," *It is published in the Journal of Bangladesh Journal of MIS,* 2024.

[34] O. Kayode-Ajala, "Applications of Cyber Threat Intelligence (CTI) in financial institutions and challenges in its adoption," *Applied Research in Artificial Intelligence and Cloud Computing,* vol. 6, no. 8, pp. 1-21, 2023.

[35] M. R. I. Bhuiyan, M. R. Faraji, M. Rashid, M. K. Bhuyan, R. Hossain, and P. Ghose, "Digital transformation in SMEs emerging technological tools and technologies for enhancing the SME's strategies and outcomes," *Journal of Ecohumanism,* vol. 3, no. 4, pp. 211-224, 2024.

[36] I. Jahan, M. N. Islam, M. M. Hasan, and M. R. Siddiky, "Comparative analysis of machine learning algorithms for sentiment classification in social media text," *World J. Adv. Res. Rev,* vol. 23, no. 3, pp. 2842-2852, 2024.

[37] J. O. Coker, N. S. Uzougbo, B. B. Oguejiofor, and O. V. Akagha, "The role of legal practitioners in mitigating corporate risks in Nigeria: a comprehensive review of existing literature on the strategies and approaches adopted by legal practitioners in Nigeria to mitigate corporate risks," *Finance & Accounting Research Journal,* vol. 5, no. 10, pp. 309-332, 2023.

[38] S. Alam, M. R. Hoque, and P. Ray, "The role of technology entrepreneurship in facilitating corporate donations: a model for B2B social e-business development," in *Technology Entrepreneurship and Sustainable Development*: Springer, 2022, pp. 159-180.

[39] G. Nzeako, M. Akinsanya, O. Popoola, E. Chukwurah, C. Okeke, and I. Akpukorji, "Theoretical insights into IT governance and compliance in banking: Perspectives from African and US regulatory environments," *International Journal of Management & Entrepreneurship Research,* vol. 6, no. 5, pp. 1457-1466, 2024.

[40] P. Conti-Brown and B. D. Feinstein, "Banking on a Curve: How to Restore the Community Reinvestment Act," *Harv. Bus. L. Rev.,* vol. 13, p. 335, 2023.

[41] A. S. George, T. Baskar, and P. B. Srikaanth, "Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors," *Partners Universal International Innovation Journal,* vol. 2, no. 1, pp. 51-75, 2024.