Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6, 8437-8453
2024
Publisher: Learning Gate
DOI: 10.55214/25768484.v8i6.3816

A systematic review on information security policies in the USA banking system and global banking: Risks, rewards, and future trends

Md Wali Ullah[1], Md. Tanvir Alam[2], Tanzina Sultana[3], Md. Mahfuzur Rahman[4*], Mahfujur Rahman Faraji[5], Md Faysal Ahmed[6]

[1]Information Technology, Westcliff University, Irvine, United States of America; M.Ullah.117@westcliff.edu (M.W.U.)
[2]Client Service Manager, Wealth & Retail Banking, Standard Chartered Bank, Dhaka, Bangladesh; tanviralamrony@gmail.com (M.T.A.).
[3]Information Technology, School of Business, Emporia State University, Emporia, United States; tsultana@g.emporia.edu (T.S.).
[4]Department of Management Information Systems, University of Dhaka, Dhaka-1000, Dhaka, Bangladesh; mahfuzmahfuz28@gmail.com (M.M.R.)
[5]Master of Science in Engineering Management, Department of Engineering Management, Westcliff University, Irvine, California, United States of America; m.faraji.214@westcliff.edu (M.R.F.)
[6]Masters of Business Administration, Westcliff University, Irvine, California, United States; m.ahmed.2594@westcliff.edu (M.F.A.).

Abstract: This study aims to examine the current state of information security policies and practices in the United States banking sector while drawing comparisons to global banking systems. The research specifically addresses risks, benefits, and future trends, providing insights for strengthening information security frameworks worldwide. The study adopts a qualitative research approach, utilizing secondary data sources, including scholarly journals, research articles, televised news, and online platforms. A systematic review was conducted using global databases such as Science Direct, Scopus, Web of Science, PubMed, DOAJ, and Google Scholar in alignment with the PRISMA 2020 guidelines. The research incorporated specific keyword phrases to identify relevant literature, with additional exclusion criteria applied to eliminate incomplete, inconsistent, or non-English publications. The final review included 125 papers and 20 reports. The findings highlight that the U.S. banking sector faces a dynamic landscape of cybersecurity risks, including phishing attacks, ransomware, regulatory non-compliance, and insider threats. Despite these risks, robust information security frameworks offer significant rewards, such as improved customer trust, fraud detection through AI and machine learning, and financial stability. The study underscores the regulatory landscape in the U.S., particularly frameworks like the Gramm-Leach-Bliley Act and collaboration initiatives such as the CISA and FS-ISAC, which enhance preparedness against emerging cyber threats. Comparative analysis with global banking systems revealed key challenges, including the evolving cyber threat landscape, compliance with international data privacy standards, and the need for cross-border cooperation. While the U.S. banking system demonstrates a strong regulatory foundation, the study identifies areas requiring improvement, such as proactive employee training, adoption of advanced cybersecurity technologies, and international cooperation. The study's implications emphasize the need for proactive risk management and continual innovation to address emerging threats. Recommendations include implementing multi-factor authentication, leveraging AI and blockchain technologies, and prioritizing cybersecurity awareness programs for employees. However, limitations include reliance on secondary data, which may omit recent developments, and a focus on the U.S. context, limiting global generalizability. Future research should incorporate primary data collection and expand the scope to include quantitative analyses of cybersecurity investments and outcomes. This research provides policymakers, banking regulators, and industry stakeholders with actionable insights to bolster information security resilience and adapt to the rapidly evolving financial landscape.

* Correspondence: mahfuzmahfuz28@gmail.com

Keywords: *Cybersecurity risks, Data protection, Global banking, Information security, Information systems, PRISMA, Security policy, Systematic review, U.S. banking.*

1. Introduction

In the contemporary financial landscape, information security has emerged as a cornerstone for the sustainability and reliability of the global banking sector (Allioui et al., 2023). Among all industries, banking institutions are arguably the most vulnerable to cyberattacks due to the highly sensitive nature of the data handle. In United States, a nation at the forefront of global financial services, ensuring robust information security measures in the banking sector is both a regulatory requirement and a necessity to maintain public trust and economic stability (Hassan et al., 2024). This research delves into the intricacies of information security in the U.S. banking sector. Since the onset of this century in the United States, information security breachers have acquired an unparalleled capacity to adversely affect organizations reputation, profitability, customer trust, and overall economic growth within the banking industry (Challoumis & Eriotis, 2024). Information security has become a universal language not only inside the global banking sector, but also across numerous other businesses particularly in the United States (Alawida et al., 2023).

According to Temara (2024), this research indicates that that although shops have been the primary targets of recent cybercrime, a significant bank in New York City experienced a breach of its computer servers by cybercriminals in the U.S. The bank disclosed that the cyber breach had jeopardized customer's data encompassing names, residential addresses, telephone numbers, and email addresses across multiple sectors; however, (Gibson & Harfield, 2023) there was no indication that the compromised data did not contain account numbers, passwords, social security numbers, or birth dates, nor was there any indication of customer fraud stemming from the breach (Albshaier et al., 2024). As global banking data became increasingly accessible via the internet and financial information became interconnected worldwide, sabotage lost its appeal; consequently, cybercriminals shifted their focus to acquiring and selling information form corporate servers (Aslan et al., 2023). The data saved on the business computer spans from innocuous information to personal datils that can facilitate identity theft (Shahriare Satu et al., 2023).

Challoumis & Eriotis (2024) said that it is essential to clarify the nature of these changes, specifically in relation to the pre-crisis characteristics of the U.S. banking system and regulatory framework. The author will examine the regulatory modifications that have arisen due to the diminishing importance of banks in external funding for enterprises and the increase in noninterest-generating activities, as well as the indistinct boundaries between banks and other depositors' institutions (Rahman et al., 2024). The individual users represent the primary vulnerability in the advancement of information security within the banking sector (Bhuiyan et al., 2024). Banks and savings & loans are recognized as financial entities that serve as stewards of their customer's personal and legacy data. Information security (IS) in global banking study has only recently acknowledged the significance of employee behavior, particularly with compliance (Allioui & Mourdi, 2023).

According to Guseva (2024), information system has emerged as the core of contemporary baking, banking information now regarded as the most precious asset to safeguard against insiders, outsiders, and competitors. Customers are highly apprehensive over privacy and identity theft in the United States (Prastyanti & Sharma, 2024). Business partners, suppliers, and vendors prioritize security as the foremost requirement (Bhuiyan et al., 2024), especially with shared network and information access (Ahmed & Khan, 2023). The capacity of banks to capitalize on new prospects frequently hinges on their ability to offer open, accessible, available, and secure network services (Hossain et al., 2024).

The predominant technological risk or threat to banks and financial institutions is phishing attacks (Uddin et al., 2024). A conventional phishing assault relies on social engineering, a strategy employed by cybercriminals to deceive individuals into disclosing sensitive information such as account usernames and passwords (Hossain et al., 2024). Armed with these credentials the fraudster can infiltrate networks, embezzle funds, and commandeer accounts. Alternative attack methods, such as spyware, trojan horses, and keyloggers, might lead a user to inadvertently download malware designed with the nefarious aim of gathering diverse personal information (Ayeni et al., 2024). Empirical research in information security governance in the U.S. is observed to be deficient, with most computer security methodologies and regulations having developed from case studies, anecdotal evidence, and the recommendations of industry "leaders". Nevertheless, managing information security based on such anecdotes is impractical in the global banking sector (Dwivedi et al., 2023).

This table summarizes the research gaps, providing an overview of the purposes, methodologies, implications, and citations of each referenced paper (Riaj et al., 2025). The focus is on addressing cybersecurity and information security in the banking sector, highlighting regulatory challenges, technological advancements, and risk management strategies (Rahman et al., 2024).

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 & 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 & 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 & 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 & Gopalkrishnan	To explore how private asset reconstruction companies	Case study, qualitative	Highlights the role of private asset management in

DOI: 10.55214/25768484.v8i6.3816

(2024)	influence financial stability.		ensuring the financial stability and cybersecurity of banking systems.

Based on the research gaps, here are two precise research objectives:

RO 1: To examine the existing information security policies and practices within the U.S. banking sector, highlighting associated risks, benefits, and their overall influence on the financial system.

RO 2: To evaluate the U.S. banking information security framework in comparison to global banking systems, identifying significant trends, challenges, and insights for strengthening information security worldwide.

2. Literature Review

According to Javaid and others (2023), information security the banking sector's significance is vital due to the sensitive nature of the data handled. The USA, being a global financial hub, faces unique challenges in this domain. Cyber threats pose a significant risk to US banks, with hackers targeting customer data and financial assets (Familoni & Shoetan, 2024). To combat these threats, banks allocate substantial resources to comprehensive security protocols, encompassing encryption, firewalls, and intrusion detection systems (Riaj et al., 2025). Regulatory compliance is another key aspect of information security in US banking (Rahman et al., 2024). Institutions must adhere to stringent regulations like the Gramm-Leach- Bliley Act and the Federal Information Security Management Act, which mandate data protection and risk management practices (Nzeako et al., 2024).

2.1. Information Security & Policy

Information Security involves safeguarding information by reducing associated risk. It constitutes a component of information risk management (Alshurideh et al., 2023). It generally entails mitigating or diminishing the probability of illegal or incorrect data access, together with criminal utilization and disclosure, interruption, deletion, corruption, modification, inspection, recording, or devaluation of information. An information security policy comprises the regulations, standards, policies, and procedures implemented by the organization to ensure the security of its IT systems (Rakha, 2023). The credibility of an organization's whole information privacy program depends on a precisely designed information security framework program relies on a meticulously crafted information security policy (Faraji et al., 2024). Numerous experts now contend that formulating an information security policy is one of the most effective methods to safeguard protected systems and assert that "the establishment of an information security policy is the initial step in equipping an organization to defend against internal and external threats" (AL-Hawamleh, 2024). They established a process for information security policy that organizations may utilize to create and assess their existing programs (Mimi et al., 2022).

2.2. The United States Information Security Scenario

In an age where digital connectedness fosters innovation, stimulates economic progress, and intertwines national security with a precarious foundation, the US President has prioritized information security in the policy agenda (Pereira & Viola, 2024). The administration's approach to information security in banking is a vital response to the threats and challenges posed by an increasingly linked digital world (Bhuiyan et al., 2024). The US information security framework maintains a precarious equilibrium between privacy and security (Mabaso & Booi, 2024). For the ruling Democratic Party, the preservation of private rights is paramount. Occasionally, such compulsions conflict with national security priorities, as the intelligence community's access to private sector networks is deliberately restricted to protect individual privacy (Gulyamov & Raimberdiyev, 2023). Banking has evolved into a global enterprise, transcending the confines of national borders. The swift expansion of foreign banks in the USA prompted heightened political pressure to curtail their growth. Domestic banks contended that international banks possessed numerous competitive advantages over them (Khan et al., 2023).

In the changing environment of information threats, achieving the appropriate balance between privacy and security will be crucial for US information security (Palle & Kathala, 2024). It is essential to define the nature of these changes, especially in relation to the pre-crisis characteristics of the US banking sector and regulatory framework (Mimi et al., 2022). Authors examined the regulatory changes that have arisen due to the diminished role of banks in external funding for enterprises and the increase in noninterest-generating activities, as well as the erosion of differences amid intensified banking globalizations (Riley & Shonchoy, 2020). According to Pereira & Viola (2024), bank regulators concentrated on ensuring that individual financial institutions possessed sufficient resources to avert failure yet overlooked systemic implications. The regulatory authorities of financial institutions in the United States adopted a macroprudential perspective and intensified their focus on preventing systemic failures inside the financial system (Familoni & Shoetan, 2024).

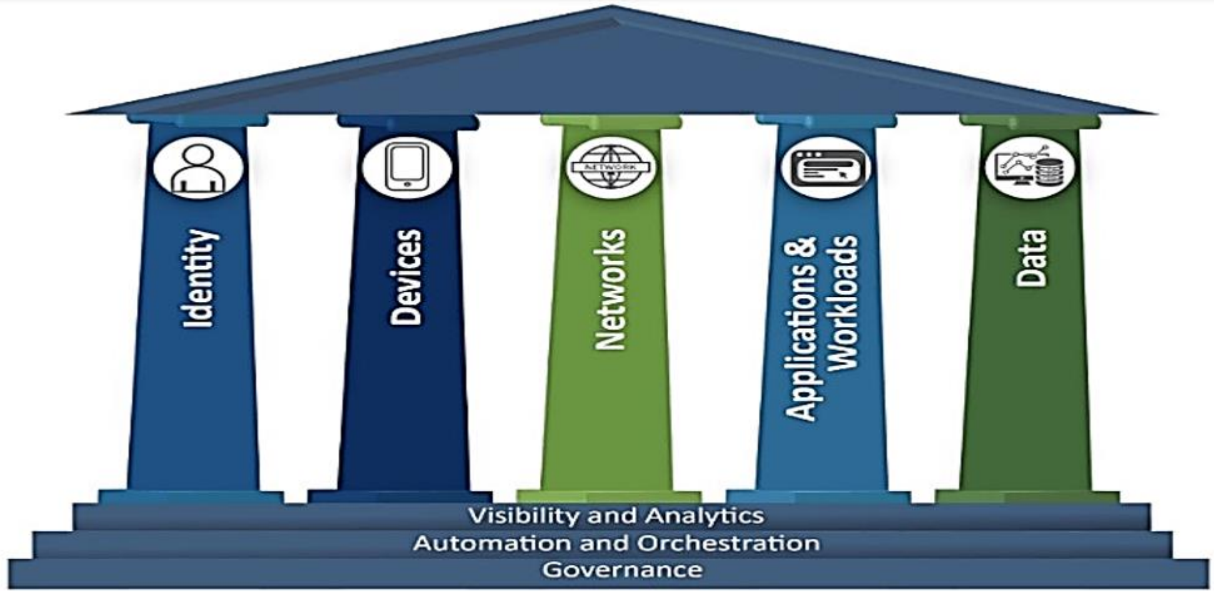


Figure 1.
US Information and infrastructure security agency.

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

In the contemporary digital era, where financial transactions occur online and sensitive information is electronically kept, cybersecurity has emerged as a significant problem for banking and financial organizations globally (Saeed et al., 2023). The significance of examining cybersecurity inside U.S. banking systems is in comprehending the unique difficulties and solutions pertinent to each nation's financial institutions (Mimi et al., 2022). A critical facet of cybersecurity within the U.S. financial sector is the necessity to combat money laundering (Akartuna et al., 2022). A group of researchers underscores the detrimental effects of money laundering on the economy and the necessity of robust measures to safeguard the banking cybersecurity framework against such activities (Bhuiyan, 2024). This underscores the importance of examining the U.S. financial sector to formulate effective cybersecurity strategies against money laundering (Bello et al., 2023). Moreover, the research provides an extensive analysis of cybersecurity frameworks and information security standards. Comprehending these guidelines and standards is essential for the U.S. banking sector to identify the most suitable cybersecurity measures that correspond with their particular needs (Khan et al., 2023).

This article is to evaluate and analyze the risks and economic implications of cybersecurity in banking and financial institutions in the United States. Cybersecurity has become a critical issue for banks and financial organizations worldwide (Hassan et al., 2024). The advancement of technology and the increasing interconnection of financial institutions have led to a troubling rise in cyber dangers. Cybersecurity protocols are essential for safeguarding the integrity and privacy of banking and financial institutions in the U.S. (Uddin et al., 2020). The study of the banking systems in the United States is significant due to its impact on the global economy. These nations possess substantial financial sectors that are essential to global trade and investment. Comprehending cybersecurity risks and economic ramifications within banking systems is crucial for policymakers, regulators, and industry experts to adeptly tackle the changing threat environment and formulate resilient cybersecurity policies (Dwivedi et al., 2023).

Table 2.
Key points about information security in worldwide banking.

Key points	Description	Reference
Evolving Threat Landscape	Emerging Hazard The landscape possesses significant authority to implement consumer protection laws applicable to both financial institutions and non-financial entities, mandating compliance with such regulations by banks with US assets exceeding a specified threshold and their affiliates, as well as certain non-financial organizations. With digital transformation accelerating worldwide, banks are increasingly adopting advanced technologies such as cloud computing, AI and blockchain. While these innovations enhance efficiency and customer experience, and also expand the attack surface for cybercriminals.	(Jaiwani & Gopalkrishnan, 2024; Kamar et al., 2023)
Regulatory Compliance	Regulatory compliance in banking necessitates that banks develop and implement policies and procedures that adhere to local and international compliance standards. Financial organizations must cultivate trust among individuals to ensure they feel secure depositing their money and assets with them. Banking institution operate in a highly regulated environment where compliance with international, regional, and national laws is critical to mitigating risk associated with data breaches, fraud, and cyberattacks.	(Adeniran et al., 2024)
Data Privacy and Protection	Data privacy and protection are critical in global banking to safeguard sensitive customer information from breaches, fraud, and cyberattacks. Banks employ encryption, secure authentication, and robust compliance measures like GDPD and CCPA to ensure data integrity and confidentiality. With increasing digitization, advanced technologies like AI and blockchain are enhancing security framework. Protecting customer trust and adhering to international regulations remain pivotal for maintaining secure financial ecosystems worldwide.	(Wang et al., 2024)
International Cooperation	International cooperation in information security is essential for worldwide banking to address cyber threats and safeguard financial systems. Collaborative efforts enable banks to share threat intelligence, establish global security standards, and respond swiftly to breaches. Organizations like financial action task force (FATF) and SWIFT facilitate secure data exchange and combat fraud. Such alliances strengthen resilience, protect customer data, and ensure trust in an increasingly interconnected financial ecosystem amidst evolving cyber risks.	(Hassan et al., 2024)

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

According to Huang & Madnick (2020), the U.S. banking sector faces a dynamic landscape of information security risk and rewards, shaped by rapid technological advancements and an evolving threat environment (Alam et al., 2024). Cybersecurity threats such as ransomware attacks, phishing schemes and insider risk are among the most significant challenges (Bhuiyan, 2024). With vast amounts of sensitive customer data and financial information stored digitally, banks are prime targets for cybercriminals seeking monetary gain or to disrupt critical infrastructure (Adeniran et al., 2024). One prominent risk is the risk of sophisticated ransomware attacks, which can cripple banking operations and result in massive financial and reputational losses (Kamar et al., 2023). Additionally, phishing campaigns targeting employees and customers often exploit human error to gain unauthorized access to systems. Regulatory non-compliance also poses risk, as failure to adhere to stringent laws such as the Gramm-Leach-Bliley Act (GLBA) or PCI DSS can lead to penalties (Faraji et al., 2024).

However, addressing these risks effectively offers significant rewards by investing in robust information security programs, U.S. banks can build customer trust, a critical asset in a competitive industry (Masud et al., 2024). Advanced technology, technologies like AI and machine learning improve fraud detection and explanation potentiality, mitigating potential damages (AL-Hawamleh, 2024). A well-secured banking system also attracts more investors and fosters long-term stability in financial markets. Collaboration with government agencies and international organizations is another rewarding strategy (Familoni & Shoetan, 2024). Initiatives like the Cybersecurity and Infrastructure Security Agency (CISA) and Financial Services Information Sharing and Analysis center (FS-ISAC) help banks share intelligence, improve defense, and prepare for emerging threats (Kayode-Ajala, 2023). In this research, a proactive approach to information security not only reduce vulnerabilities but also positions United States as leaders in safeguarding financial data (Adeniran et al., 2024). By balancing risk management with innovation, banks can ensure secure operations while adapting to an increasingly digital financial ecosystem.

3. Methodology

This study primarily adopts a qualitative research approach, relying extensively on secondary data sources. These sources include scholarly journals, research papers, televised news reports, and online platforms (Khanom et al., 2022). The study seeks to explore the existing information security policies and practices within the U.S. banking sector, emphasizing the associated risks, rewards, and their broader implications on the financial system (Bhuiyan et al., 2024). Additionally, the research aims to evaluate the U.S. banking information security framework in relation to global banking systems, identifying key trends, challenges, and insights to enhance information security on a worldwide scale (Rahman et al., 2024).

The data search process utilized renowned global databases, including Science Direct, Scopus, Web of Science, PubMed, DOAJ, and Google Scholar, adhering to the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) 2020 guidelines. PRISMA provides a standardized framework for systematically documenting and reporting research findings, particularly in reviews and meta-analyses based on robust evidence (Khatun et al., 2025). Although PRISMA predominantly focuses on randomized trials with a database size of 2520 datasets (Jahan et al., 2024), it also offers a structured methodology for reporting systematic reviews across other research domains, including non-therapeutic evaluations. Ensuring a transparent and thorough account of systematic review methodologies and results allows readers to assess the reliability and relevance of the findings (Hossain et al., 2024).

The research process incorporated specific keyword phrases such as “comparison to global banking systems,” “identifying significant trends,” “challenges,” and “insights for strengthening information security worldwide” to align with the study’s objectives. Records that did not match the predefined keywords or subject focus were excluded (Islam et al., 2024). Additional exclusion criteria included insufficient data availability, publications in languages other than English, inconsistent outcomes, and studies with fragmented findings (Mani, 2024). Following a rigorous screening process, researchers identified 125 additional papers and 20 reports, as presented in Figure 2.

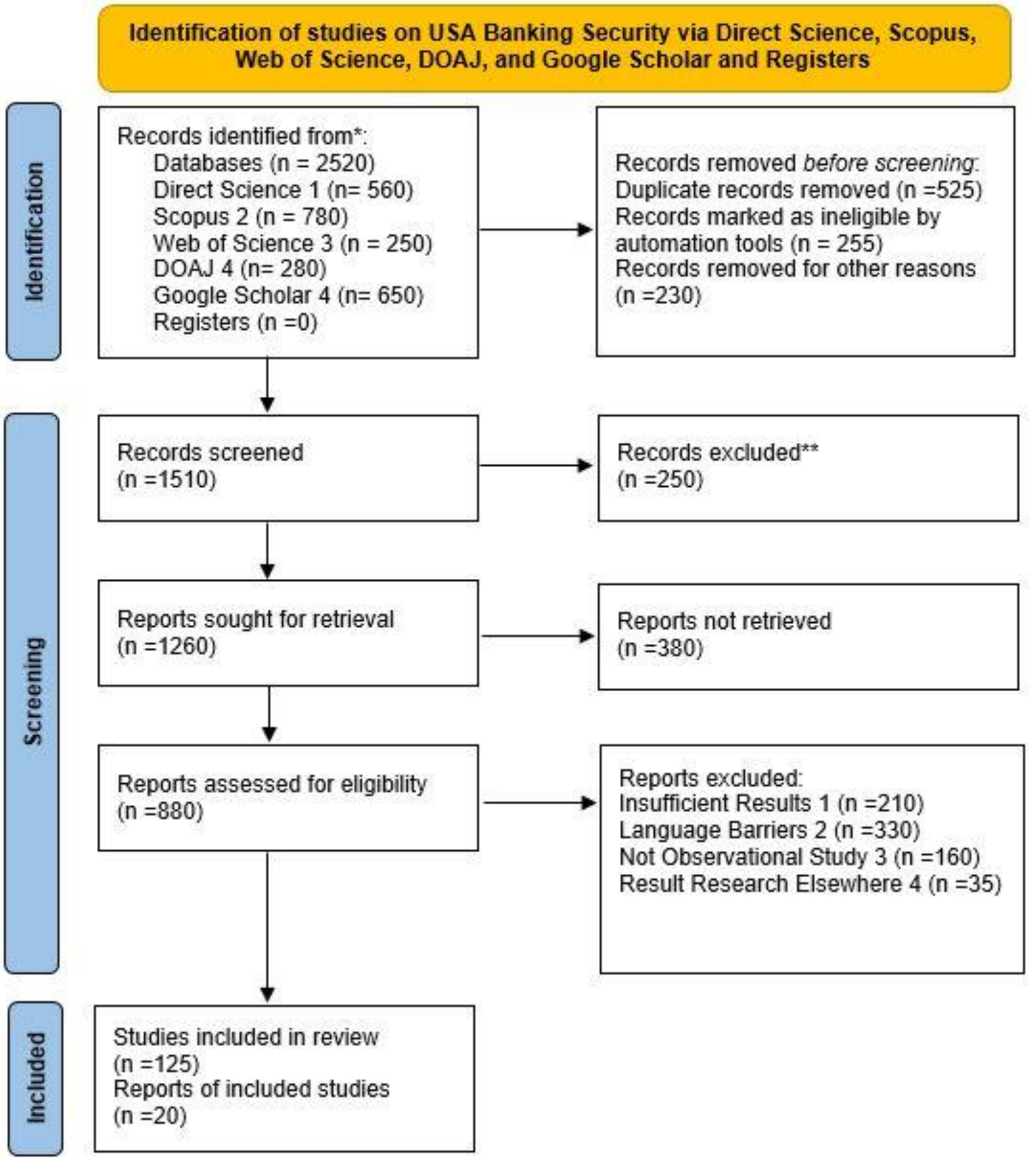

Identification of studies on USA Banking Security via Direct Science, Scopus, Web of Science, DOAJ, and Google Scholar and Registers
Identification
Records identified from*:
Databases (n = 2520)
Direct Science 1 (n= 560)
Scopus 2 (n = 780)
Web of Science 3 (n = 250)
DOAJ 4 (n= 280)
Google Scholar 4 (n= 650)
Registers (n =0)
Records removed *before screening*:
Duplicate records removed (n =525)
Records marked as ineligible by automation tools (n = 255)
Records removed for other reasons (n =230)
Screening
Records screened (n =1510)
Records excluded** (n =250)
Reports sought for retrieval (n =1260)
Reports not retrieved (n =380)
Reports assessed for eligibility (n =880)
Reports excluded:
Insufficient Results 1 (n =210)
Language Barriers 2 (n =330)
Not Observational Study 3 (n =160)
Result Research Elsewhere 4 (n =35)
Included
Studies included in review (n =125)
Reports of included studies (n =20)

Figure 2.
Systematic review methodology.

4. Discussion

4.1. U.S. Banking and Financial Landscape

According to Coker et al. (2023), the U.S. banking and financial environment is defined by competitiveness, risk management, monetary policy transmission, and the function of financial intermediaries. Examine the mechanisms for averting bank runs and maintaining market liquidity, highlighting the critical functions of deposit insurance and liquidity (Fungacova et al., 2021). Their discourse highlights the need for regulatory measures in maintaining stability within the U.S. banking system (Alam et al., 2022). Examining the influence of financial development on risk-taking and risk distribution. The extension of the financial sector's borders has introduced greater risk exposure and improved access to borrowing (Ayeni et al., 2024). This development has revealed additional concerns, especially the susceptibility to disruptions caused by the banking industry (Bhuiyan et al., 2024). This comprehension is essential for maintaining stability within the U.S. banking sector (Elnahass et al., 2021).

This research examines the U.S. banking and financial sector, offering insights into competition, risk management, monetary policy transmission, and the function of financial intermediaries (Dang, 2020). These studies enhance the understanding of the dynamics and difficulties inside the U.S. banking system, facilitating effective policymaking and risk management.

4.2. Information Security in Worldwide Banking

The International Banking Act, enacted in 1978, subjected foreign bank units operating in the U.S. to the oversight of American authorities and the FDIC (Gortsos, 2023). Before the Act, U.S. branches of foreign banks were governed by a fragmented array of state-specific laws (Khan et al., 2023). Numerous experts contend that information security awareness (ISA) is a critical component for attaining the objectives of information security within enterprises. An Information Security Awareness (ISA) program is characterized as a condition in which individuals inside an organization possess awareness of, and ideally demonstrate commitment to, their security objectives (Nzeako et al., 2024). The ISA is temporary and requires frequent renewal, particularly within businesses in the banking sector, which adhere to this guidance by consistently "refreshing" relevant ISAs in accordance with stringent ISPs. The utilized internal channels for information acquisition may encompass traditional methods, instructor-led techniques, and digital platforms (Mabaso & Booi, 2024). A recent global case study on a large international bank with various locations revealed that standard methods included internal newspapers, pamphlets, posters, and printed coffee cups.

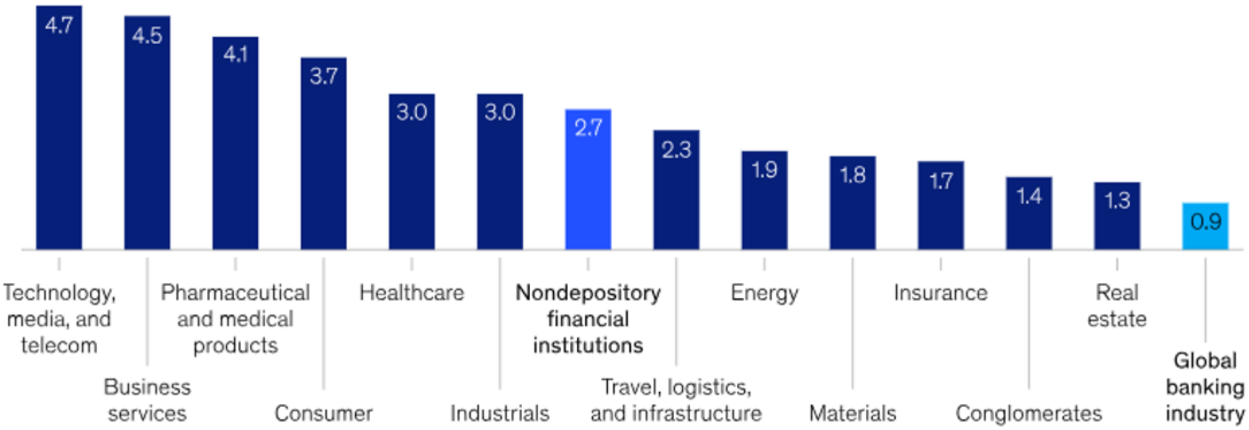
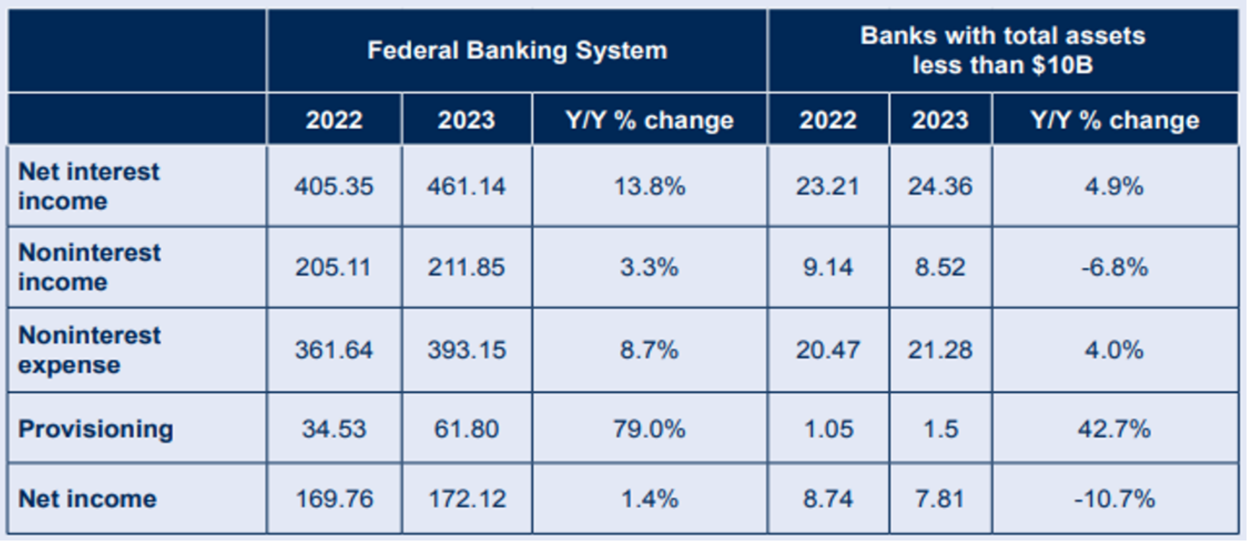


Figure 3.
Price-to-Book ratio, by industry, 2023.
Source: McKinsey Panorama; McKinsey value Intelligence.

Mandatory instructor-led workshops were conducted for staff induction, focusing on compliant information security behavior in accordance with the bank's Information Security Policy (ISP) (Kamar et al., 2023). Digital methods were executed and disseminated through the intranet, which served as the primary communication medium for notifications and e-learning initiatives, as well as an online repository for accessing the ISP. Evolving Threat Landscape, Regulatory Compliance, Data Privacy and Protection, and International Cooperation are the key points about Information Security in Worldwide Banking (Pereira & Viola, 2024).



	Federal Banking System			Banks with total assets less than $10B		
	2022	2023	Y/Y % change	2022	2023	Y/Y % change
Net interest income	405.35	461.14	13.8%	23.21	24.36	4.9%
Noninterest income	205.11	211.85	3.3%	9.14	8.52	-6.8%
Noninterest expense	361.64	393.15	8.7%	20.47	21.28	4.0%
Provisioning	34.53	61.80	79.0%	1.05	1.5	42.7%
Net income	169.76	172.12	1.4%	8.74	7.81	-10.7%

Figure 4.
Trends in bank net income (In Billions).
Source: Call reports from OCC integrated banking information system.

4.3. Recommendations for Strengthening Cybersecurity in Banking

The growing importance of cybersecurity in the banking and financial sectors, particularly in the U.S., highlights the pressing necessity for strong measures to mitigate possible threats and vulnerabilities (Riggs et al., 2023). Based on the insights and findings from the preceding sections, the following detailed recommendations are presented to enhance cybersecurity in the banking sector:

Proactive Cybersecurity Measures: Financial organizations must emphasize the adoption of proactive cybersecurity strategies. This involves the implementation of multi-factor authentication, the development of a resilient digital infrastructure, and the execution of regular security evaluations to identify and address vulnerabilities prior to exploitation (Safitra et al., 2023).

Continuous Employee Training: Human errors frequently represent the most vulnerable aspect of cybersecurity. Organizations must allocate substantial resources to ongoing employee training and awareness initiatives (Abrahams et al., 2024). Regular training sessions must be established to ensure workers remain informed about the latest threats, potential weaknesses, and optimal countermeasures (Adeniran et al., 2024).

Adoption of Cybersecurity Frameworks: Financial institutions ought to proactively implement and modify recognized cybersecurity procedures. These frameworks offer a methodical strategy for addressing cybersecurity risks and may be tailored to address the unique requirements of any enterprise (Kaur et al., 2023).

Embrace Technological Innovations: As technology rapidly evolves in the financial sector, institutions must leverage sophisticated technologies to strengthen their cybersecurity measures (Efijemue et al., 2023). This involves implementing artificial intelligence and machine learning for immediate threat identification and employing blockchain technology to guarantee transactional security (Yazdinejad et al., 2023).

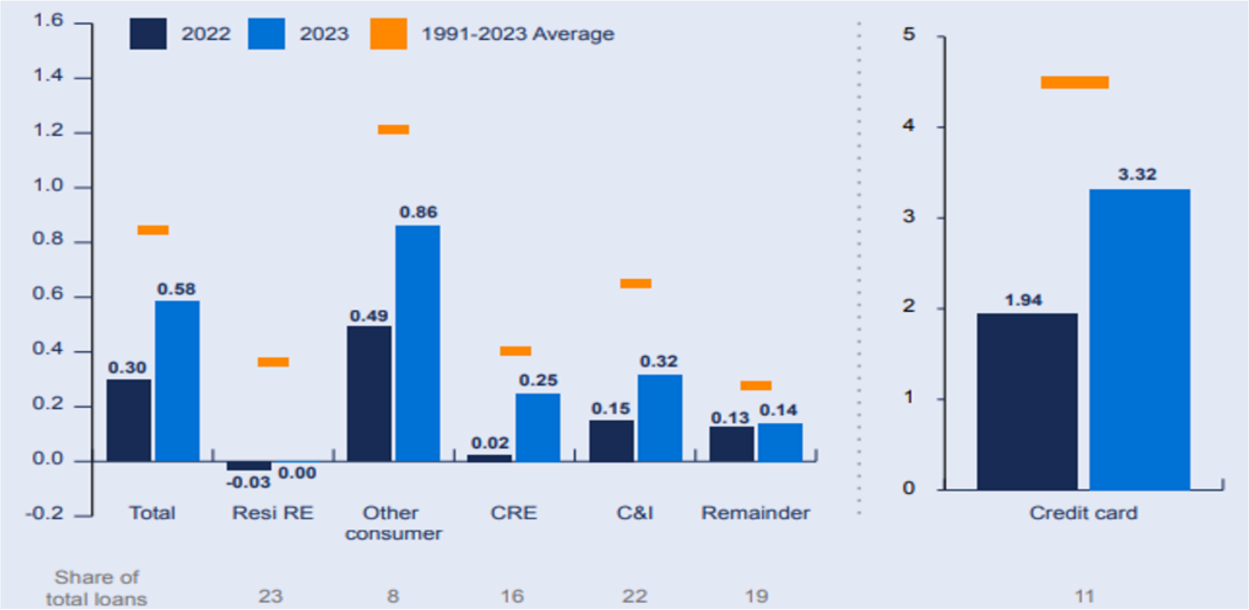


Figure 5.
Net charge-off rates for the federal banking system.
Source: Call Reports from OCC integrated banking information system.

4.4. Implementation of Cybersecurity Policies and Procedures

According to George et al. (2024) said that bank supervision and internal governance by the OCC emphasize (1) implementing essential security risk management procedures and controls to safeguard against cyber threats, together with robust response programs and operational resilience capabilities to mitigate and minimize the effects of a cybersecurity incident. The operating plan for bank supervision of the OCC for Fiscal Year 2024 prioritizes operational resilience and cybersecurity for national banks, federal savings associations, federal branches, federal agencies, and third-party service providers (Teng et al., 2023).

Table 3.
Oversight and supervision of support cybersecurity.

Item	Description	Reference
Systemic Risk Identification and Support (SyRIS)	The SyRIS division identifies, evaluates, and collaborates with both intra- and interagency partners to comprehensively assess and mitigate risks affecting the OCC's mission regarding supervision. It offers subject matter expertise across all risk domains, aids in resource prioritization, and directly supervises services rendered by major service providers.	(Conti-Brown & Feinstein, 2023)
Bank Supervision Policy (BSP)	The BSP operates three policy divisions dedicated to operational resilience and cybersecurity threats: The Bank Information Technology Policy section creates and maintains cybersecurity supervision guidance, resources, examination guides, and supervisory tools, including the FFIEC IT Examination Handbook and related work programs. Critical Infrastructure Policy examines systemic operational risks that could degrade or disrupt the federal banking system and cause national economic issues. The organization also coordinates internal responses and information exchange during critical infrastructure situations like cybersecurity. The Governance and Operational Risk Policy unit promotes risk-based supervision and provides advice on governance and operational risk for OCC. This involves addressing current and new hazards, supporting examiners with uniform interpretation, creating educational resources, and doing internal and external outreach.	(Hassan et al., 2024; Pereira & Viola, 2024; Kamar et al., 2023)
The Office of Financial Technology	The OCC serves as the central clearinghouse for federal banking system innovation inquiries and information. OCC outreach and engagement with banks and financial technology companies on new or innovative federal banking products, services, and technologies is coordinated by this unit. New or innovative products, services, and technologies may require operational resilience and cybersecurity cooperation.	(Vijayagopal et al., 2024; Saeed et al., 2023)

In comparison to global banking systems, the U.S. stands out in terms of its regulatory approach, but also faces unique challenges related to the rapid pace of technological advancements and the evolving cyber threat landscape (Bhuiyan et al., 2023). Key global trends include the growing significance of data privacy and protection, the integration of new technologies such as blockchain, and the increasing need for international cooperation in combating cybercrime. The study highlights the importance of developing comprehensive cybersecurity strategies that are adaptable to both domestic and global financial ecosystems. Despite the strengths of the U.S. banking system, this research identifies several areas for improvement. Proactive cybersecurity measures, including the implementation of multi-factor authentication and regular employee training programs, are essential to reduce human error and strengthen defenses. Additionally, the study underscores the need for banks to embrace cutting-edge technologies and adopt cybersecurity frameworks that can be tailored to their unique requirements.

5. Conclusions

This study provides a comprehensive analysis of the information security landscape within the U.S. banking sector, examining both the current practices and their implications, as well as drawing comparisons with global banking systems (Khatun et al., 2024). Through the application of qualitative research methods and a systematic review of secondary data sources, the study uncovers significant insights into the challenges, risks, rewards, and future trends in banking cybersecurity. The findings confirm that information security is a critical concern for the U.S. banking system, with the sector being particularly vulnerable to cyber threats such as phishing attacks, ransomware, and insider threats (Bhuiyan et al., 2024). While these risks pose considerable challenges, the rewards of robust cybersecurity frameworks are substantial. U.S. banks that invest in advanced security technologies, such as artificial intelligence and machine learning, can mitigate these risks, build customer trust, and enhance financial stability. Furthermore, regulatory compliance plays a pivotal role in safeguarding sensitive financial data, with institutions adhering to frameworks like the Gramm-Leach-Bliley Act and collaborating with agencies such as CISA and FS-ISAC to improve resilience against emerging threats (Hossain et al., 2024).

This research offers several implications for policymakers and banking regulators. It provides actionable recommendations for improving cybersecurity resilience in the financial sector, particularly the need for proactive risk management, continuous training, and collaboration with international counterparts. However, the study's reliance on secondary data limits its scope, and future research could benefit from incorporating primary data and quantitative analysis to further explore the relationship between cybersecurity investments and organizational outcomes. The U.S. banking sector must continue to adapt and innovate in its approach to information security, balancing regulatory requirements, emerging threats, and technological advancements to ensure the long-term stability and security of the financial system.

6. Limitations and Future Directions

This study primarily relies on secondary data sources, including scholarly articles, reports, and news broadcasts, which may present limitations in terms of timeliness and comprehensiveness. The use of secondary data restricts the ability to capture recent developments in the U.S. banking sector's information security practices, potentially overlooking the latest trends and emerging threats (Bhuiyan et al., 2024). Additionally, the study focused solely on the U.S. banking system, which may limit the generalizability of the findings to other banking sectors worldwide with different regulatory environments and cybersecurity challenges. Furthermore, the qualitative approach employed does not allow for direct measurement of the effectiveness of the policies and frameworks analyzed, nor does it provide a statistical representation of the impact of security measures across various banks (Hossain et al., 2024).

Future research should aim to incorporate primary data collection, such as surveys or interviews with banking professionals and cybersecurity experts, to gain real-time insights into the effectiveness of current information security measures and the challenges faced in implementing them (Bhuiyan et al., 2023). Quantitative studies could also be valuable in evaluating the actual performance and outcomes of information security strategies in banking, allowing for a more robust analysis of the costs and benefits of different approaches. Another potential avenue for future research is the exploration of cross-border data-sharing practices and international cooperation in tackling global cybersecurity threats, as well as the comparative effectiveness of various regulatory frameworks across regions (Islam et al., 2024). Additionally, future studies could explore the role of emerging technologies, such as artificial intelligence and blockchain, in advancing banking security and mitigating novel cyber risks (Hossain et al., 2024). Finally, more in-depth investigation into the human factor, particularly employee behavior and compliance with security protocols, could provide critical insights into strengthening the security culture within financial institutions (Masud et al., 2024).

Data Availability:

The data supporting this study are derived from secondary sources, including scholarly journals, research papers, online platforms, and news reports. These data are publicly available through global databases such as Science Direct, Scopus, Web of Science, PubMed, DOAJ, and Google Scholar.

Acknowledgement:

Authors would like to express my sincere gratitude to all the researchers, institutions, and authors whose work contributed to this study. Special thanks to the databases and resources that provided valuable data. I also appreciate the support of my mentors and colleagues for their invaluable insights and guidance throughout this research.

Copyright:

References

[1] Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., & Hassan, A. O. (2024). A review of cybersecurity strategies in modern organizations: examining the evolution and effectiveness of cybersecurity measures for data protection. Computer Science & IT Research Journal, 5(1), 1-25.

[2] Adeniran, I. A., Abhulimen, A. O., Obiki-Osafiele, A. N., Osundare, O. S., Agu, E. E., & Efunniyi, C. P. (2024). Strategic risk management in financial institutions: Ensuring robust regulatory compliance. Finance & Accounting Research Journal, 6(8), 1582-1596.

[3] Ahmed, S., & Khan, M. (2023). 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, 13(9), 1-17.

[4] Akartuna, E. A., Johnson, S. D., & Thornton, A. (2022). Preventing the money laundering and terrorist financing risks of emerging technologies: An international policy Delphi study. Technological Forecasting and Social Change, 179, 121632.

[5] Alam, S., Afrin, S., Alam, S. A., Bhuiyan, M. R. I., Galván, R. S., Martínez, A. B., & Tabassum, S. (2024). A Conceptual Framework for Family Business Strategic Direction in the Bangladeshi Readymade Garment Industry. *Bangladesh Journal of MIS*, *10*(01). http://dx.doi.org/10.61606/BJMIS.V10N1.A2

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

[7] Alawida, M., Mejri, S., Mehmood, A., Chikhaoui, B., & Isaac Abiodun, O. (2023). A comprehensive study of ChatGPT: advancements, limitations, and ethical considerations in natural language processing and cybersecurity. Information, 14(8), 462.

[8] Albshaier, L., Almarri, S., & Hafizur Rahman, M. M. (2024). A review of blockchain's role in E-Commerce transactions: Open challenges, and future research directions. Computers, 13(1), 27.

[9] AL-Hawamleh, A. (2024). Cyber resilience framework: Strengthening defenses and enhancing continuity in business security. International Journal of Computing and Digital Systems, 15(1), 1315-1331.

[10] Allioui, H., & Mourdi, Y. (2023). Exploring the full potentials of IoT for better financial growth and stability: A comprehensive survey. Sensors, 23(19), 8015.

[11] Alshurideh, M., Alquqa, E., Alzoubi, H., Kurdi, B., & Hamadneh, S. (2023). The effect of information security on e-supply chain in the UAE logistics and distribution industry. Uncertain Supply Chain Management, 11(1), 145-152.

[12] Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333.

[13] Ayeni, R. K., Adebiyi, A. A., Okesola, J. O., & Igbekele, E. (2024, April). Phishing Attacks and Detection Techniques: A Systematic Review. In 2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG) (pp. 1-17). IEEE.

[14] Bello, O. A., Folorunso, A., Onwuchekwa, J., & Ejiofor, O. E. (2023). A Comprehensive Framework for Strengthening USA Financial Cybersecurity: Integrating Machine Learning and AI in Fraud Detection Systems. European Journal of Computer Science and Information Technology, 11(6), 62-83.

[15] Bhuiyan, M. R. I. (2024). Examining the digital transformation and digital entrepreneurship: A PRISMA based systematic review. Pakistan Journal of Life and Social Sciences, 22(1), 1136-1150. http://dx.doi.org/10.57239/PJLSS-2024-22.1.0077

[16] Bhuiyan, M. R. I. (2024). Industry Readiness and Adaptation of Fourth Industrial Revolution: Applying the Extended TOE Framework, *Human Behavior and Emerging Technologies*, 8830228, 14 pages, 2024. https://doi.org/10.1155/hbe2/8830228

[17] Bhuiyan, M. R. I., Akter, M. S., & Islam, S. (2024). How does digital payment transform society as a cashless society? An empirical study in the developing economy. *Journal of Science and Technology Policy Management.* https://doi.org/10.1108/JSTPM-10-2023-0170

[18] Bhuiyan, M. R. I., Faraji, M. R., Rashid, M., Bhuyan, M. K., Hossain, R., & Ghose, P. (2024). Digital Transformation in SMEs Emerging Technological Tools and Technologies for Enhancing the SME's Strategies and Outcomes. *Journal of Ecohumanism*, *3*(4), 211-224. https://doi.org/10.62754/joe.v3i4.3594

[19] Bhuiyan, M. R. I., Faraji, M. R., Tabassum, M. N., Ghose, P., Sarbabidya, S., & Akter, R. (2024). Leveraging Machine Learning for Cybersecurity: Techniques, Challenges, and Future Directions. *Edelweiss Applied Science and Technology*, *8*(6), 4291-4307. https://doi.org/10.55214/25768484.v8i6.2930

[20] Bhuiyan, M. R. I., Hossain, R., Rashid, M., Islam, M. M., Mani, L., & Milon, M. N. U. (2024). Gravitating the components, technologies, challenges, and government transforming strategies for a Smart Bangladesh: A PRISMA-based review. Journal of Governance & Regulation, 13(3), 177–188. https://doi.org/10.22495/jgrv13i3art15

[21] Bhuiyan, M. R. I., Islam, M. T., Alam, S. A., & Sumon, N. S. (2023). Identifying Passengers Satisfaction in Transportation Quality: An Empirical Study in Bangladesh. *PMIS Review*, *2*(1), 27-46.

[22] Bhuiyan, M. R. I., Milon, M. N. U., Hossain, R., Poli, T. A., & Salam, M. A. (2024). Examining the Relationship between Poverty and Juvenile Delinquency Trends in a Developing Country. *Academic Journal of Interdisciplinary Studies*, *13*(6), 255-274. DOI: https://doi.org/10.36941/ajis-2024-0193

[23] Bhuiyan, M. R. I., Uddin, K. S., & Milon, M. N. U. (2023). Prospective Areas of Digital Economy: An Empirical Study in Bangladesh. doi: 10.20944/preprints202307.1652.v1

[24] Challoumis, C., & Eriotis, N. (2024). A historical analysis of the banking system and its impact on Greek economy. Edelweiss Applied Science and Technology, 8(6), 1598-1617.

[25] Coker, J. O., Uzougbo, N. S., Oguejiofor, B. B., & Akagha, O. V. (2023). 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, 5(10), 309-332.

[26] Conti-Brown, P., & Feinstein, B. D. (2023). Banking on a Curve: How to Restore the Community Reinvestment Act. Harv. Bus. L. Rev., 13, 335.

[27] Dang, V. D. (2020). The conditioning role of performance on the bank risk-taking channel of monetary policy: Evidence from a multiple-tool regime. Research in International Business and Finance, 54, 101301.

[28] Dwivedi, Y. K., Kshetri, N., Hughes, L., Slade, E. L., Jeyaraj, A., Kar, A. K., ... & Wright, R. (2023). 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, 71, 102642.

[29] Efijemue, O., Obunadike, C., Taiwo, E., Kizor, S., Olisah, S., Odooh, C., & Ejimofor, I. (2023). Cybersecurity strategies for safeguarding customers data and preventing financial fraud in the United States financial sectors. International Journal of Soft Computing, 14(3), 10-5121.

[30] Elnahass, M., Trinh, V. Q., & Li, T. (2021). Global banking stability in the shadow of Covid-19 outbreak. Journal of International Financial Markets, Institutions and Money, 72, 101322.

[31] Familoni, B. T., & Shoetan, P. O. (2024). Cybersecurity in the financial sector: a comparative analysis of the USA and Nigeria. Computer Science & IT Research Journal, 5(4), 850-877.

[32] Faraji, M. R., Shikder, F., Hasan, Md. H., Islam, Md. M., & Akter, U. K. (2024). Examining the Role of Artificial Intelligence in Cyber Security (CS): A Systematic Review for Preventing Prospective Solutions in Financial Transactions. International Journal of Religion, 5(10), 4766–4782. https://doi.org/10.61707/7rfyma13

[33] Fungacova, Z., Turk, R., & Weill, L. (2021). High liquidity creation and bank failures. Journal of Financial Stability, 57, 100937.

[34] George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. Partners Universal International Innovation Journal, 2(1), 51-75.

[35] Gibson, D., & Harfield, C. (2023). Amplifying victim vulnerability: Unanticipated harm and consequence in data breach notification policy. International Review of Victimology, 29(3), 341-365.

[36] Gortsos, C. V. (2023). The European Banking Regulation Handbook, Volume I. Springer Books.

[37] Gulyamov, S., & Raimberdiyev, S. (2023). Personal data protection as a tool to fight cyber corruption. International Journal of Law and Policy, 1(7).

[38] Guseva, Y. (2024). Decentralized Markets and Decentralized Regulation. George Washington Law Review.

[39] Hassan, A. O., Ewuga, S. K., Abdul, A. A., Abrahams, T. O., Oladeinde, M., & Dawodu, S. O. (2024). Cybersecurity in banking: a global perspective with a focus on Nigerian practices. Computer Science & IT Research Journal, 5(1), 41-59.

[40] Hossain, F., Ahmed, G. M. S., Shuvo, S. P. P., Kona, A. N., Raina, M. U. H., & Shikder, F. (2024). Unlocking artificial intelligence for strategic market development and business growth: innovations, opportunities, and future directions. *Edelweiss Applied Science and Technology*, *8*(6), 5825–5846. https://doi.org/10.55214/25768484.v8i6.3263

[41] Hossain, R., Al- Amin, A.-A., Mani, L., Islam, M. M., Poli, T. A., & Milon, M. N. U. (2024). Exploring the Effectiveness of Social Media on Tourism Destination Marketing: An Empirical Study in a Developing Country. WSEAS TRANSACTIONS ON BUSINESS AND ECONOMICS, 21, 1392–1408. https://doi.org/10.37394/23207.2024.21.114

[42] Hossain, R., Ghose, P., Chowdhury, T. M., Hossen, M. D., Hasan, M. N., & Mani, L. Ownership Structures and Firm Performance: A Correlation and Regression Analysis of Financial Institutions in Bangladesh. *Pak. j. life soc. Sci.*, *22*(2): 6278-6295. https://doi.org/10.57239/PJLSS-2024-22.2.00473

[43] Hossain, R., Sohag, H. J., Farhatul, H., Ahmed, S., Amin, A.-, & Islam, Md. M. (2024). Prospective Artificial Intelligence (AI) Applications in the University Education Level: Enhancing Learning, Teaching and Administration through a PRISMA Base Review Systematic Review. Pakistan Journal of Life and Social Sciences (PJLSS), 22(2). https://doi.org/10.57239/PJLSS-2024-22.2.00694

[44] Huang, K., & Madnick, S. (2020). Cyber securing cross-border financial services: calling for a financial cybersecurity action task force. *Available at SSRN 3544325.*

[45] Islam, M. A., Fakir, S. I., Masud, S. B., Hossen, M. D., Islam, M. T., & Siddiky, M. R. (2024). Artificial intelligence in digital marketing automation: Enhancing personalization, predictive analytics, and ethical integration. *Edelweiss Applied Science and Technology*, *8*(6), 6498-6516. DOI: 10.55214/25768484.v8i6.3404

[46] Jahan, I., Islam, M. N., Hasan, M. M., & Siddiky, M. R. (2024). Comparative analysis of machine learning algorithms for sentiment classification in social media text. *World J. Adv. Res. Rev*, *23*(3), 2842-2852. https://doi.org/10.30574/wjarr.2024.23.3.2983

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

[48] Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. Cyber Security and Applications, 1, 100016.

[49] Kamar, E., Howell, C. J., Maimon, D., & Berenblum, T. (2023). The moderating role of thoughtfully reflective decision-making on the relationship between information security messages and smishing victimization: An experiment. Justice Quarterly, 40(6), 837-858.

[50] Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, 101804.

[51] Kayode-Ajala, O. (2023). Applications of Cyber Threat Intelligence (CTI) in financial institutions and challenges in its adoption. Applied Research in Artificial Intelligence and Cloud Computing, 6(8), 1-21.

[52] Khan, H. H., Khan, S., & Ghafoor, A. (2023). Fintech adoption, the regulatory environment and bank stability: An empirical investigation from GCC economies. Borsa Istanbul Review, 23(6), 1263-1281.

[53] Khatun, M., Hossain, R., Bhuiyan, M. R. I., Tabassum, M. N., & Riaj, M. A. J. (2025). Green Entrepreneurship and Digital Transformation for Sustainable Development: A Systematic Review. *Digitizing Green Entrepreneurship*, 153-180. DOI: 10.4018/979-8-3693-7442-9.ch006

[54] Khatun, M., Islam, R., Kumar, S., Hossain, R., & Mani, L. (2024). The Impact of Artificial Intelligence on Educational Transformation: Trends and Future Directions. *Journal of Information Systems and Informatics*, *6*(4), 2347-2373. https://doi.org/10.51519/journalisi.v6i4.879

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

[56] Mani, L. (2024). Gravitating towards the Digital Economy: Opportunities and challenges for transforming smart Bangladesh. *Pakistan Journal of Life and Social Sciences*, *22*(1), 3324-3334. https://doi.org/10.57239/PJLSS-2024-22.1.00241

[57] Masud, S. B., Rana, M. M., Sohag, H. J., Shikder, F., Faraji, M. R., & Hasan, M. M. Understanding the Financial Transaction Security through Blockchain and Machine Learning for Fraud Detection in Data Privacy and Security. Pak. j. life soc. Sci. (2024), 22(2): 17782-17803. https://doi.org/10.57239/PJLSS-2024-22.2.001296

[58] Masud, S. B., Siddiky, M. R., Chowdhury, S. A., Rohan, A., & Rahaman, M. A. (2024). Navigating Role Identity Tensions: It Project Managers' Identity Work in Agile Information Systems Development. *European Journal of Technology*, *8*(6), 1-16.

[59] Mimi, A., Imran, M. A., Beg, T. H., & Rahman, M. S. (2022). Governmental and Institutional Initiatives And Actions For The Attraction And Expansion Of E-Commerce By Women In Bangladesh. *American Economic & Social Review*, *9*(1), 17-28. https://doi.org/10.46281/aesr.v9i1.1733

[60] Mimi, A., Imran, M. A., Mustafa, J., Beg, T. H., & Rahman, M. S. (2022). Efforts by Women to Become Financially Independent Through E-Commerce During Covid-19: A Study on Bangladesh Perspective. *American Economic & Social Review*, *9*(1), 9-16. https://doi.org/10.46281/aesr.v9i1.1723

[61] Nzeako, G., Akinsanya, M. O., Popoola, O. A., Chukwurah, E. G., Okeke, C. D., & Akpukorji, I. S. (2024). Theoretical insights into IT governance and compliance in banking: Perspectives from African and US regulatory environments. International Journal of Management & Entrepreneurship Research, 6(5), 1457-1466.

[62] Palle, R. R., & Kathala, K. C. (2024). Balance between security and privacy. Privacy in the Age of Innovation, 129-135. https://doi.org/10.1007/979-8-8688-0461-8_11

[63] Pereira, J. C., & Viola, E. (2024). From protagonist to laggard, from pariah to phoenix: Emergence, decline, and re-emergence of Brazilian climate change policy, 2003–2023. Latin American Policy, 15(3), 400-422.

[64] Prastyanti, R. A., & Sharma, R. (2024). Establishing Consumer Trust Through Data Protection Law as a Competitive Advantage in Indonesia and India. Journal of Human Rights, Culture and Legal System, 4(2), 354-390.

[65] Rahman, M. M., Bhuiyan, M. R., & Alam, S. M. (2024). The Empirical Study on the Impact of the COVID-19 on Small and Medium Enterprises (SMEs) in Bangladesh. *Journal of Information Systems and Informatics*, *6*(1), 527-547. https://doi.org/10.51519/journalisi.v6i1.686

[66] Rahman, M. M., Kshetri, N., Sayeed, S. A., & Rana, M. M. (2024). AssessITS: Integrating procedural guidelines and practical evaluation metrics for organizational IT and Cybersecurity risk assessment. *arXiv preprint arXiv:2410.01750*. https://doi.org/10.48550/arXiv.2410.01750

[67] Rakha, N. A. (2023). Ensuring Cyber-security in Remote Workforce: Legal Implications and International Best Practices. International Journal of Law and Policy, 1(3).

[68] Riaj, M. A. J., Tabassum, M. N., Hossain, R., Bhuiyan, M. R. I., & Khatun, M. (2025). Digitalization Transformation in Entrepreneurship and Enterprise Green Innovation. In *Digitizing Green Entrepreneurship* (pp. 181-204). IGI Global Scientific Publishing. DOI: 10.4018/979-8-3693-7442-9.ch007

[69] Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., ... & Sarwat, A. I. (2023). Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. Sensors, 23(8), 4060.

[70] Riley, E., & Shonchoy, A. (2020). The role of mobile banking for small and Microenterprises amid the COVID-19 crisis in Ghana. AEA Randomized Controlled Trials. https://doi.org/10.1257/rct.6275

[71] Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. Sensors, 23(15), 6666.

[72] Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. Sustainability, 15(18), 13369.

[73] Shahriare Satu, M., Yeasmin, T., & Abdus Salam, M. (2023, December). Towards an AutoML-Based Data Analytical Framework for Predicting Bankruptcy in Industrial Sector. In *International Conference on Trends in Electronics and Health Informatics* (pp. 699-712). Singapore: Springer Nature Singapore.

[74] Temara, S. (2024). The Ransomware Epidemic: Recent Cybersecurity Incidents Demystified. Asian Journal of Advanced Research and Reports, 18(3), 1-16.

[75] Teng, H. W., Härdle, W. K., Osterrieder, J., Baals, L. J., Papavassiliou, V. G., Bolesta, K., ... & Orhun, E. (2023). Mitigating digital asset risks.

[76] UDDIN, K. S., BHUIYAN, M. R. I., & HAMID, M. (2024). Perception towards the Acceptance of Digital Health Services among the People of Bangladesh. *WSEAS Transactions on Business and Economics*, *21*:1557-1570 https://doi.org/10.37394/23207.2024.21.127

[77] Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. Risk Management, 22(4), 239-309.

[78] Vijayagopal, P., Jain, B., & Ayinippully Viswanathan, S. (2024). Regulations and Fintech: A Comparative Study of the Developed and Developing Countries. Journal of Risk & Financial Management, 17(8).

[79] Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. Computers & security, 147, 104051.

[80] Yazdinejad, A., Dehghantanha, A., Parizi, R. M., Srivastava, G., & Karimipour, H. (2023). Secure intelligent fuzzy blockchain framework: Effective threat detection in iot networks. Computers in Industry, 144, 103801.