International Journal of Information Science and Computing
Citation: *IJISC*: **12**(01): 31-48, June 2025
DOI: 10.30954/2348-7437.1.2025.4

INFORMATION SCIENCE AND TECHNOLOGY FOUNDATION

REVIEW PAPER

A Comprehensive Analysis of Cyber-security Risks in Digital Banking and Their Socio-economic Impacts

Md Asaduzzaman[1], Prosannajid Sarkar[2*], Nahid Reza Shatu[3] and Anima Barma[4]

[1]*Researcher, National University, Bangladesh*
[2]*Institute of Research Excellence, Begum Rokeya University Rangpur, Bangladesh*
[3]*Researcher, National University, Bangladesh*
[4]*Govt. Begum Rokeya College, Rangpur, Bangladesh*

**Corresponding author: drpsarkarwri@gmail.com*

Received: 10 Apr., 2025 **Revised:** 21 May, 2025 **Accepted:** 01 June, 2025

ABSTRACT

The swift digitisation of banking services has transformed financial accessibility while simultaneously increasing vulnerability to cyber threats, resulting in significant socio-economic repercussions. This mixed-methods study examines the evolving landscape of cyber-security threats in digital banking, encompassing phishing, ransomware, malware, data breaches, insider threats, and DDoS attacks. It assesses their impact on institutions, customers, and the economy. A quantitative analysis of a decade-long dataset indicates a marked increase in cyber incidents, with reported attacks on financial institutions escalating from 1,500 in 2019 to 3,348 in 2023, accompanied by considerable economic disruptions, including GDP contractions (–1% to –2%), surges in unemployment (+2.8 percentage points), and a decline in customer trust (–45%). Qualitative views from cyber-security experts, policymakers, and financial regulators underscore organisational and regulatory hurdles in addressing these threats. The study introduces the CUBE Security Model, which incorporates Continuous AI-driven detection, Unified threat intelligence, Blockchain-secured transactions, and Encrypted cloud-based protection, in conjunction with advanced technologies such as zero-trust architectures, quantum-resistant encryption, and decentralised identity systems. Comparative case studies highlight regional differences in cyber-security resilience, emphasizing the importance of governance and innovation in maintaining socio-economic stability. This research integrates cyber-security with socio-economic analysis to provide practical frameworks that enhance digital banking resilience, foster public trust, and promote global financial stability in an interconnected environment. The swift digitisation of banking services has transformed financial accessibility while simultaneously revealing significant vulnerabilities to cyber threats. This report analyses the changing cyber-security threats in digital banking and their extensive socio-economic impacts on organisations, customers, and economies.

Keywords: Cyber-security Risk, Digital Banking, Socio-Economic Impacts, Digital Financial Ecosystem, Analysis

How to cite this article: Asaduzzaman, Md., Sarkar, P., Shatu, N.R. and Barma, A. (2025). A Comprehensive Analysis of Cyber-security Risks in Digital Banking and Their Socio-economic Impacts. *IJISC.*, **12**(01): 31-48.

Source of Support: None; **Conflict of Interest:** None

The advent of digital banking has revolutionized the global financial industry, transforming how individuals and businesses access financial services, conduct transactions, and invest. Digital platforms have enhanced financial inclusion and economic growth, particularly in underserved areas, by providing convenience, speed, and accessibility. As the digital banking ecosystem expands, it has become increasingly vulnerable to various cyber-security threats, including phishing attempts, ransomware, insider threats, and data breaches. These hazards jeopardize the security of financial systems and pose substantial challenges to consumer trust, economic stability, and overall socio-economic development.

Cyberattacks on financial institutions can have extensive repercussions, interrupting both individual and organisational functions while also instigating systemic shocks that affect the broader economy. The economic repercussions of extensive data breaches might erode public trust in digital banking, impeding adoption rates and obstructing financial inclusion initiatives. The swift progression of technology innovations in digital finance, along with deficiencies in cyber-security regulation, has resulted in a complex and dynamic environment where conventional risk mitigation measures frequently fall short in addressing new threats.

This study aims to provide an exhaustive examination of the cyber-security threats facing digital banking and their socio-economic consequences. This study aims to elucidate the broader implications of cyber-attacks on financial stability, consumer behavior, and social equality by examining the relationship between cyber-security vulnerabilities and their economic consequences. The project will employ a mixed-methods approach, integrating quantitative analysis of cyber event data with qualitative insights from industry experts and stakeholders, to provide a comprehensive knowledge of the problems and potential in securing digital financial ecosystems. This research aims to propose pragmatic policies and innovative solutions to safeguard the future of digital banking, ensuring its ongoing contribution to economic prosperity while mitigating threats to global financial institutions.

REVIEW OF LITERATURE

The advancement of digital banking has transformed the financial services sector by facilitating quicker, more efficient, and convenient transactions. This swift evolution has increased the vulnerability of economic systems to cyber-security threats. This literature review consolidates current research on cyber-security threats in digital banking and its socio-economic effects, emphasising technological advancements and resilience frameworks as possible mitigation strategies.

Cyber-security Threats in Digital Banking

The advent of digital banking has revolutionised financial services, offering convenience and efficiency. However, it also exposes consumers and organisations to increasing cyber-security threats, such as phishing, malware, and data breaches. Insufficient authentication, system vulnerabilities, and human error amplify these risks. Enforcing rigorous security protocols is vital for safeguarding sensitive financial data and maintaining trust in digital banking systems.

Phishing and Social Engineering Attacks: Phishing and social engineering attacks continue to be among the most prevalent cyber-security concerns in digital banking. Research conducted by Alsharif *et al.* (2020) highlights how attackers exploit human vulnerabilities to gain unauthorized access to sensitive data. Progress in artificial intelligence has facilitated the development of advanced phishing methods, rendering detection increasingly more challenging.

Malicious Software and Ransomware: Kaspersky's research (2021) cites malware and ransomware as significant threats to digital banking. These assaults often involve malicious software designed to disrupt networks, steal data, or compromise systems for financial gain. Banking Trojans, including Dridex and Emotet, primarily target online banking systems.

Data Breaches: Data breaches pose a significant risk, as research indicates a consistent increase in both the frequency and severity of these incidents. The Ponemon Institute's "Cost of a Data Breach Report" (2022) indicates that financial organisations incur above-average breach costs owing to the sensitivity of their data.

Insider Threats: Both deliberate and inadvertent insider threats represent a significant concern. The research conducted by Cappelli *et al.* (2019) emphasises the importance of comprehensive employee training programs and rigorous access restrictions to reduce these hazards. Individuals with privileged access may inadvertently or intentionally jeopardise important information, resulting in substantial financial and reputational damage.

Distributed Denial of Service (DDoS) attacks can impede banking operations by inundating servers with excessive traffic. According to research by Cloudflare (2022), the banking industry is one of the most frequently targeted industries for DDoS attacks, often resulting in reputational harm and significant economic losses.

Socio-economic Consequences of Cyber-security Threats

Financial Losses: Cyber-security breaches in digital banking can result in significant economic detriment for both organisations and clients. The 2021 IBM "Cost of a Data Breach Report" puts the average expense of a breach in the banking sector at $5.72 million, excluding reputational harm and indirect losses.

Trust Deficiency: Customer trust constitutes a fundamental element of digital banking. Deloitte's studies (2021) demonstrate that cyber-security breaches substantially undermine trust, resulting in customer loss and a decline in the uptake of digital banking services.

Regulatory and Legal Consequences: Cyber-security incidents often result in increased regulatory oversight. Basu's (2020) research highlights that institutions must comply with developing legislation, including the GDPR, CCPA, and PSD2, which often leads to additional compliance costs and penalties for non-compliance.

Economic Inequality: Cyber-security threats disproportionately impact lower-income consumers who depend on digital banking for accessible financial services. Research, such as that conducted by the World Bank (2020), highlights that these vulnerabilities exacerbate economic inequality, particularly in emerging economies.

Economic Performance and Employment: The Financial Consequences of Cyber-security Breaches Beyond the Banking Sector. Anderson and Moore (2021) assert that effective cyber-attacks frequently disrupt supply chains, resulting in significant economic repercussions, including employment reductions and reduced GDP growth. The financial strain of recuperation intensifies these problems.

Strategies for Mitigation

Technological Solutions: Research highlights the necessity of using sophisticated security solutions, including multi-factor authentication (MFA) and biometric verification.

Blockchain Technology: Blockchain has surfaced as a viable alternative for enhancing the security of digital finance. Nakamoto (2008) originally devised blockchain to enhance cryptocurrencies, but its utility in safe and transparent financial transactions has subsequently broadened. Research by Zhang *et al.* (2020) highlights the blockchain's capacity to eliminate single points of failure, enhance transparency, and foster trust within financial systems.

Artificial Intelligence (AI) and Machine Learning (ML) are revolutionary technologies in the field of cyber-security. Wang *et al.* (2022) examine how AI-driven predictive analytics might proactively detect abnormalities and potential dangers, facilitating preventive measures. These technologies enhance fraud detection systems by learning and adapting to evolving patterns of cyber-attacks.

Zero-Trust Architecture: Zero-trust frameworks emphasize authentication at every access point. Forrester Research (2021) emphasizes the growing implementation of zero-trust frameworks in financial institutions to reduce risks associated with conventional perimeter-based security. This method guarantees that all access requests, regardless of origin, are meticulously verified.

Collaborative initiatives among financial institutions are essential for addressing cybercrime. The Financial Services Information Sharing and Analysis Centre (FS-ISAC) serves as a prominent forum for banks to exchange threat intelligence and best practices.

Policy and Regulation: Governments and regulatory agencies play a crucial role in addressing cyber-security concerns. ISO (2022) recommends the implementation of harmonised international standards and frameworks to guarantee uniformity in cyber-security procedures globally. Governments and regulatory agencies have established numerous frameworks to tackle cyber-security issues. The European Union's General Data Protection Regulation (GDPR) and the United States' Cyber-security Information Sharing Act (CISA) have played a crucial role in establishing data protection standards and facilitating the sharing of information.

Staff Development: Human mistake continues to be a substantial contributor to cyber-security breaches. According to ENISA (2021), training programs can enable staff to identify and mitigate potential dangers.

Public Awareness Initiatives: Enhancing public knowledge on cyber-security threats is essential. Campaigns emphasising secure online practices, as advised by the UK's National Cyber Security Centre (NCSC), can mitigate risks at the individual level.

Lacuna

Cyber-security threats in digital banking pose substantial problems with profound socio-economic consequences. Despite much research in this domain, some gaps persist that necessitate additional investigation:

- ❒ Assessing the indirect expenses associated with cyber-security breaches.
- ❒ Analyzing the influence of new technologies, including quantum computing, on the security of digital banking.
- ❒ Investigating the contribution of public-private partnerships to the enhancement of cyber-security resilience.

Cyber-security threats in digital banking pose substantial problems with extensive socio-economic consequences. Mitigating these hazards requires a comprehensive strategy that encompasses technical

advancements, public education, and regulatory oversight. Moreover, concerns about data privacy often hinder the dissemination of crucial cyber-security information due to conflicts with privacy laws and company regulations. By addressing research deficiencies and promoting collaboration, stakeholders may alleviate risks and guarantee the secure and inclusive advancement of digital banking. Addressing these research gaps is crucial for enhancing the security of digital banking systems and mitigating their socio-economic impacts. An integrated strategy that incorporates technological advancements, regulatory transparency, and targeted socio-economic policies is crucial to protect the digital banking ecosystem.

Research Objectives

This study primarily aims to investigate various cyber-security threats in digital financial systems, encompassing phishing, ransomware, data breaches, disruptions to banking operations, client data compromises, and erosion of trust in digital platforms. The subsequent section delineates the principal research aims of the study:

1. To evaluate the effects of cyber-security threats.
2. To analyze the socio-economic effects.
3. To formulate strategic solutions and provide new, practical frameworks for ensuring the security of digital banking while promoting socio-economic growth.

Methods and Methodology

This study utilizes a mixed-methods approach, integrating quantitative and qualitative methodologies to thoroughly examine cyber-security concerns in digital banking and their socio-economic effects. The research design incorporates empirical data analysis and key informant interviews. This rigorous technique guarantees a thorough and practical examination of cyber-security vulnerabilities in digital banking, encompassing both technological and socio-economic aspects. The study framework shown below delineates the comprehensive methodological procedures.

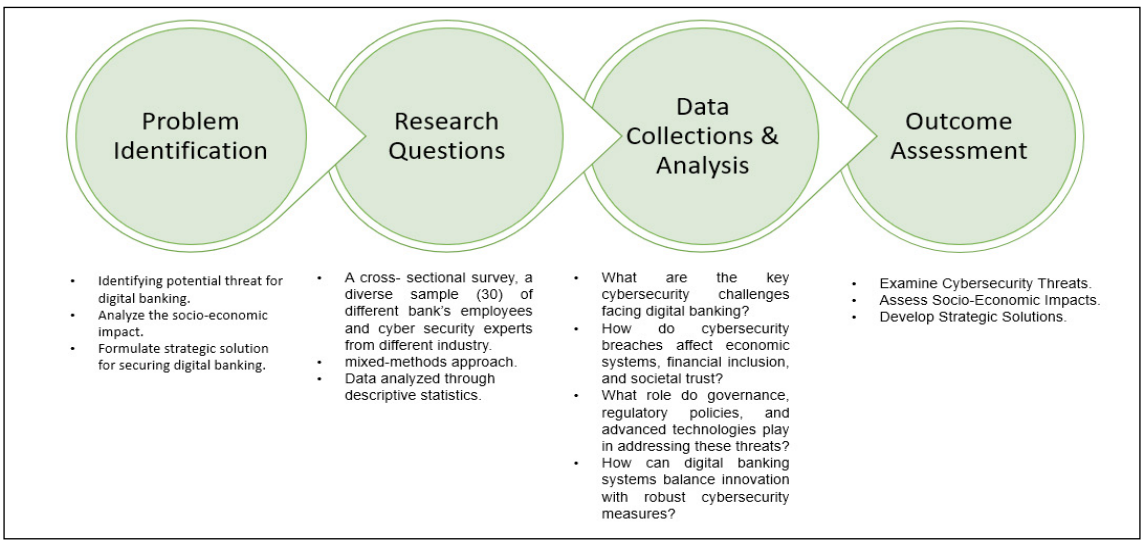

Fig. 1: Research Framework for the Study

DATA COLLECTION METHODS

Quantitative Data Collection

Collect data on cyber-attacks targeting financial institutions over the past decade, including attack types, frequency, economic losses, and recovery timelines. The study utilises macroeconomic indicators, such as GDP and banking metrics, to analyse cyber-security threats and their correlation with financial market volatility and transaction volumes.

Qualitative Data Collection

Conduct semi-structured interviews with key informants, such as cyber-security professionals, banking executives, policy advisors, and economists. Analyze cyber-security incidents across regions to identify best practices in the banking industry.

Data Analysis

A combination of statistical analysis and thematic analysis is employed. Quantitative data from surveys and reports are analyzed using statistical tools to determine patterns and trends in cyber-security threats, financial losses, and consumer behavior. Qualitative data from interviews and case studies are analyzed thematically to identify recurring issues, challenges, and the broader socio-economic consequences of digital banking cyber threats.

RESULTS AND DISCUSSION

Key Cyber-security Challenges Facing Digital Banking

Digital banking has revolutionized the financial industry by providing convenience and efficiency. However, with this advancement comes an increased risk of cyber threats. Financial institutions must address various cyber-security challenges to protect customer data, maintain trust, and comply with regulatory requirements.

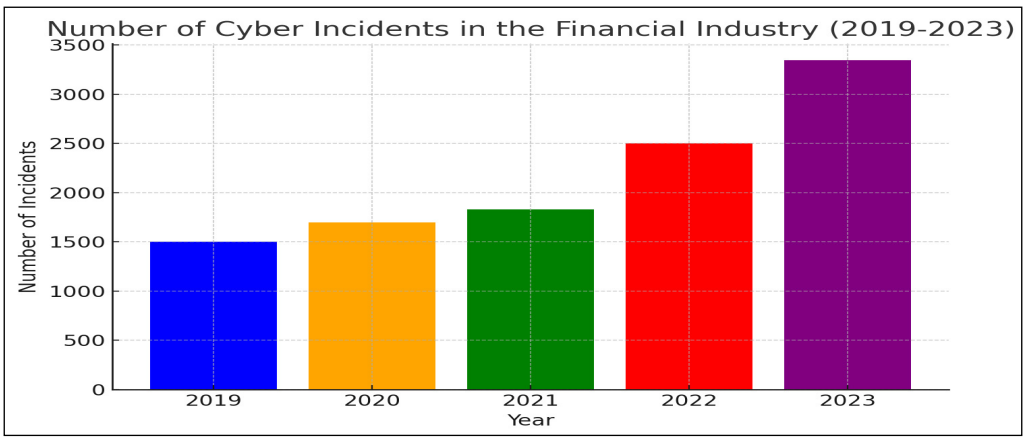

Fig. 2: Continuous Rise in Cyber Incidents Affecting Financial Institutions

Over the past five years, the banking industry has witnessed a substantial rise in cyber-attacks, with various types of threats becoming increasingly prevalent. Below is a bar diagram illustrating the number of reported cyber incidents in the financial sector from 2019 to 2023.

The financial sector reported approximately 1,500 cyber incidents in 2019, which increased to 1,700 in 2020. This period marked the beginning of a noticeable rise in cyber threats targeting financial institutions. In 2021, the number of reported incidents reached 1,829. This increase can be attributed to the growing sophistication of cybercriminals and the expanded attack surface due to digital transformation in banking services. The upward trend continued in 2022, with reported incidents rising to 2,500. The surge is linked to the increased adoption of online banking services, which, while convenient, also present more opportunities for cyber-attacks. A significant spike occurred in 2023, with 3,348 reported cyber incidents. This represents the highest number of attacks in the past decade, highlighting the escalating threat landscape.

Table 1: Cyber-security challenges in digital banking

Challenge	**Description**
Phishing & Social Engineering	Deceptive tactics to steal user credentials and financial information.
Malware & Ransomware	Malicious software that steals data or locks systems until a ransom is paid.
Insider Threats	Risks from employees, contractors, or vendors misusing access.
Data Breaches & Privacy Concerns	Unauthorised access to sensitive customer data can result in both financial and reputational damage.
DDoS Attacks	Large-scale cyber-attacks that disrupt online banking services.

Table 1 outlines key cyber-security challenges and their explanations. Phishing & Social Engineering – Scammers trick people into revealing sensitive information, such as passwords or banking details, by pretending to be trustworthy entities.

Malware & Ransomware – Harmful software that either steals data or locks computer systems until a ransom is paid to regain access. Insider Threats – Risks caused by employees, contractors, or vendors who misuse their access to systems, either intentionally or accidentally. Data Breaches & Privacy Concerns – Unauthorized access to sensitive customer data can result in financial loss and damage to a company's reputation. DDoS (Distributed Denial of Service) Attacks – Large-scale cyber-attacks that overload and disrupt online services, making them unavailable to users. These challenges underscore the importance of robust security measures in protecting sensitive information and maintaining trust in digital services.

Fig. 3 illustrated that the frequency distribution of cyber-security risks from 0 to 100. Malware, Ransomware, Phishing/Smishing, DoS Attacks, and Data Breaches are risks. At 24%, phishing and smishing attacks are the most significant cyber-security threats. Cybercriminals use fake emails, messages, and websites to steal login credentials and financial information. SMS smishing occurs instead of email phishing. With its high frequency, enterprises must prioritize user awareness and deploy strong email and message filtering. As the second most common danger, malware accounts for 23% of events. Malware encompasses viruses, worms, trojans, and spyware that harm, disrupt, or gain illegal access to systems. Malicious email attachments, software downloads, and infected websites spread malware. Phishing emails often deliver malware; thus, the near-equal rate indicates that both attacks are linked. Unauthorized access to personal data accounts for 22% of cyber-security incidents. Due to cyber-attacks, weak security, or

insider threats, customer data, trade secrets, and financial information are leaked. Data breaches can result in significant economic losses, regulatory penalties, and reputational damage.

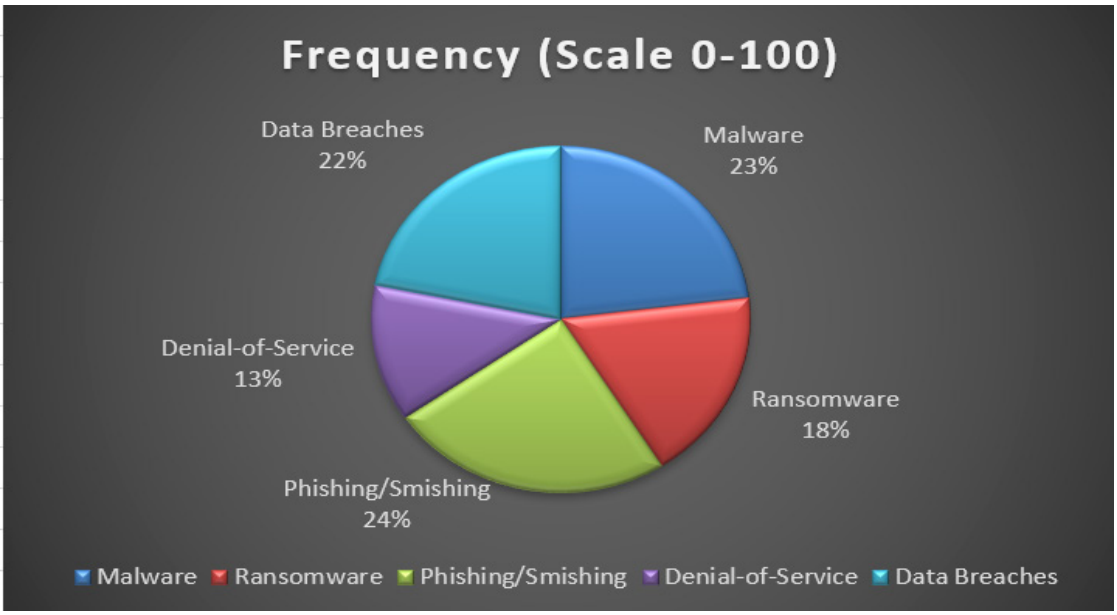

Fig. 3: Frequency (0-100) of Different Cyber Threats

Ransomware accounts for 18% of cyber-security issues. This spyware seeks a ransom to decrypt data. Phishing emails and vulnerabilities in outdated software are often used to spread ransomware. The lower rate than general malware implies that not all malware infections result in ransomware attacks, but its financial and operational impact remains a significant problem. The lowest DDoS Frequency Service attacks are the smallest, at 13%. Attacks flood systems, networks, and websites with traffic, making services unavailable to legitimate users. DoS assaults are the least frequent threat, but they can impair financial institutions.

Analysis of Cyber Attack Types, Frequency, Financial Losses, and Recovery Time

In the digital age, cyber threats have become increasingly sophisticated, targeting individuals, businesses, and government institutions. Understanding the various types of cyber-attacks, their frequency, estimated financial losses, and recovery times is crucial for developing effective cyber-security strategies.

Table 2 shows that the rapid growth of digital and internet banking has made financial institutions and consumers more convenient and accessible. Cyber threats have increased due to this expansion, making cyber-security a significant concern for the financial sector. This research presents statistics and trends that link the expansion of digital banking to an increase in cyber-attacks. Online transactions have increased due to the adoption of mobile and digital banking, rendering financial institutions increasingly vulnerable to cyber-attacks. The table below lists the main cyber-attack types affecting digital banking, along with their frequency, anticipated financial damages, and recovery timelines. The data highlights the evolving threat landscape and the economic costs of cyber-security breaches.

This research examines six major kinds of cyber-attacks—phishing, ransomware, data breaches, DDoS attacks, insider threats, and malware infections—analyzing their impact on cyber-security and financial stability. Table 2 represented Cyber Attack Types, Frequency, Financial Losses, and Recovery Time.

Table 2: Cyber Attack Types, Frequency, Financial Losses, and Recovery Time

Cyber Attack Type	Frequency of Attacks	Estimated Financial Loss ($)	Average Recovery Time (Days)
Phishing Attacks	High	500M+	3-5
Ransomware	Moderate	1B+	7-14
Data Breaches	High	2B+	10-30
DDoS Attacks	Moderate	750M+	5-10
Insider Threats	Low	300M+	15-25
Malware Infections	High	600M+	3-7

The report indicates that phishing is a prevalent cyber threat, frequently perpetrated through misleading emails, messages, or websites intended to deceive victims into disclosing personal information, including login passwords and financial data. Phishing attacks are prevalent due to their simplicity and commonality in cybercrime. The projected financial detriment from phishing surpasses $500 million, primarily attributable to identity theft, fraudulent purchases, and compromised corporate accounts. The typical recovery duration for phishing incidents spans from 3 to 5 days, as firms must reset compromised accounts, enhance security protocols, and instruct personnel to avert future assaults. Ransomware is a type of malware that encrypts the files of its victims, requiring payment (often in cryptocurrency) for the decryption key. These attacks transpire with low regularity yet result in catastrophic financial repercussions, with projected losses exceeding $1 billion worldwide. The financial repercussions stem from ransom payments, operational disruptions, and legal expenses. Recovering from ransomware can be arduous, typically requiring 7 to 14 days, depending on the severity of the encryption, the effectiveness of backup systems, and the victim's decision to pay the ransom.

Data breaches involve unauthorised access to confidential information, often affecting millions of individuals and organisations. The frequency of these attacks is elevated due to the growing dependence on digital storage and cloud computing. Financial damages from data breaches surpass $2 billion, mostly attributed to regulatory penalties, reputational harm, and expenses related to notifying impacted individuals and enhancing security protocols. Recovery from a data breach typically requires 10 to 30 days; however, enduring consequences may last for years, affecting customer trust and corporate operations. DDoS assaults entail inundating a target system with enormous traffic, hence incapacitating it for genuine users. These attacks occur with considerable regularity, frequently targeting large corporations, financial institutions, and government agencies. The financial repercussions of DDoS attacks are estimated to be $750 million, primarily due to operational downtime, revenue loss, and the costs of mitigation. The recovery phase typically requires 5 to 10 days, contingent upon the magnitude of the attack and the efficacy of countermeasures, such as traffic filtering and server redundancy. Insider threats, in contrast to external attacks, arise from workers, contractors, or business associates who exploit their access rights to misappropriate or corrupt data. These dangers are less common than external cyber-attacks but can be very detrimental due to their challenging detection. The projected financial loss due to insider threats amounts to $300 million, including fraud, intellectual property theft, and regulatory fines. Recovery

from insider attacks typically requires 15 to 25 days, as firms must investigate the breach, restrict access privileges, and implement stricter access controls. Malware, encompassing viruses, worms, and Trojans, represents a persistent cyber-security threat that spreads through malicious software downloads, email attachments, and compromised websites. Malware infections are prevalent, resulting in financial losses of $600 million attributed to data corruption, system repair, and diminished productivity. The recovery duration for malware infections varies from 3 to 7 days, depending on the complexity of the infection and the effectiveness of cyber-security protocols, including antivirus software and network monitoring.

Trends of Different Cyber-Attacks in Digital Banking Over the Last Five Years

The study highlights the increasing frequency of cyber threats targeting online financial services. Key cyber-attacks, including malware, phishing, ransomware, DDoS, and data breaches, have shown a steady rise, with ransomware witnessing the most significant growth. Phishing and malware attacks remain persistent threats, exploiting user vulnerabilities to steal credentials. DDoS attacks disrupt banking services, while data breaches compromise sensitive financial information. The upward trend underscores the need for enhanced cyber-security measures, robust fraud detection systems, and effective regulatory policies to safeguard digital banking against evolving cyber threats.

Fig. 4 illustrates the developments in various categories of cyber-attacks from 2019 to 2023, encompassing malware, phishing, ransomware, DDoS attacks, and data breaches. There is a distinct upward trajectory in cyber threats over the years, with ransomware attacks experiencing the most significant increase, particularly since 2021. Phishing and malware attacks have increased steadily, while DDoS attacks and data breaches have exhibited a consistent upward trend. The research underscores the escalating cyber-security concerns, highlighting the need for enhanced defensive measures to combat these increasingly advanced threats.

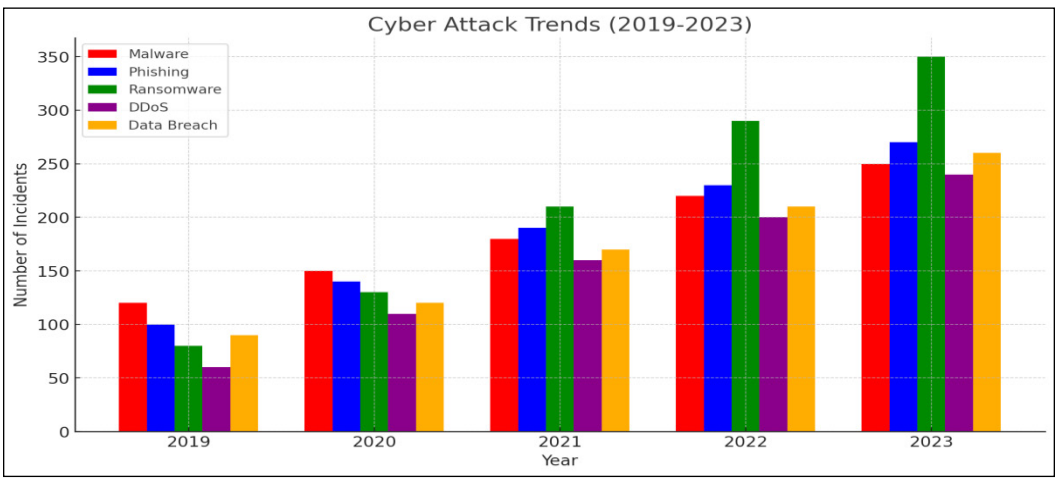

Fig. 4: Cyber Attack Trends (2019-2023)

Assess the socio-economic consequences of various categories of cyber risks

Cyber threats in digital banking and various industries have substantial socio-economic repercussions, affecting individuals, enterprises, and governments. This study examines the far-reaching impacts of

cyber-security threats on digital banking across four dimensions: economic, social, national, and global. It examines significant upheavals, regulatory obstacles, and security issues that impact financial organizations and their clients globally. It underscores the necessity for proactive strategies, stricter regulations, and international collaboration to mitigate cyber threats. The following table summarizes the impact of cyber threats on the socio-economic landscape:

Table 3: A Multi-Dimensional Cyber-Threats

Category	**Key Impacts**	**Affect**
Economic Impact	Financial losses, service disruptions, and security costs	Reduced profits, high expenses
Social Impact	Loss of trust, data privacy risks, job disruptions	Reduced digital banking adoption
National Impact	Regulatory challenges, economic slowdown	Stricter policies, financial risk
Global Impact	Cross-border cybercrime, market instability	Need for global cooperation

Socio-Economic Impacts of Cyber-Threats on Digital Banking

Cyber-security threats in digital banking have substantial economic, social, national, and global ramifications, affecting financial institutions, consumers, and governments. Cyberattacks lead to financial losses, service disruptions, and increased security expenditures, ultimately diminishing profitability and escalating operational costs. Socially, these dangers erode trust in digital banking, expose users to data privacy vulnerabilities, and lead to employment interruptions, ultimately hindering adoption rates. At the national level, regulatory issues and economic downturns necessitate more stringent policies, which in turn elevate financial risks. Worldwide, transnational cybercrime and market volatility underscore the pressing necessity for international collaboration in cyber-security governance.

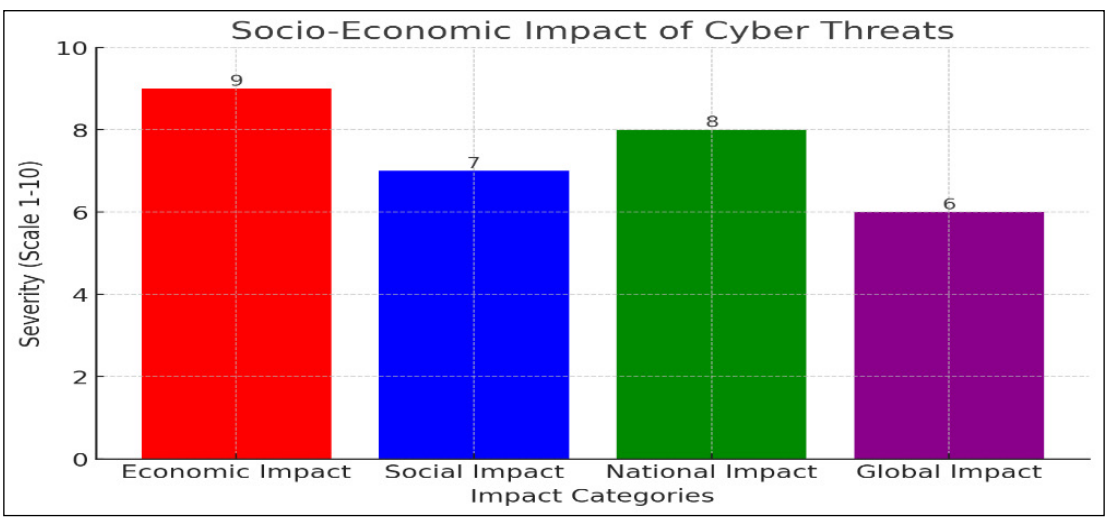

Fig. 5: Social-economic Impacts of Cyber Threats

Fig. 5 illustrated that the severity of cyber threats across four key impact categories—Economic, Social, National, and Global—on a scale from 1 to 10. The economic impact is the highest, rated at 9, indicating

that cyber threats have a significant impact on financial stability, resulting in monetary losses, increased security costs, and disrupted banking services. The National Impact, rated at 8, highlights the regulatory challenges and financial risks governments face due to cyber threats. The Social Impact, scored at 7, reflects how cyber incidents erode public trust in digital banking, increase data privacy concerns, and disrupt employment in the financial sector. The Global Impact, though relatively lower at 6, underscores the growing risks of cross-border cybercrime and financial market instability. Overall, the graph emphasizes the pressing need for stronger cyber-security frameworks and global cooperation to mitigate these severe socio-economic consequences.

How a Major Cyber-Attack Leads to Severe Unemployment

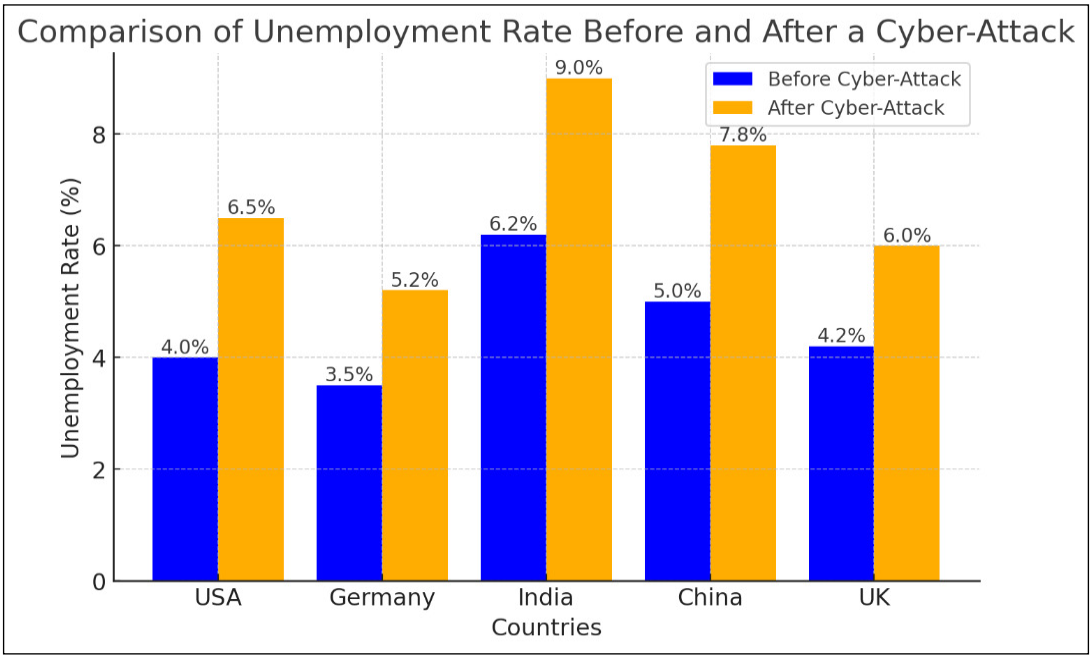

Fig. 6: Comparison of Unemployment Rate Before & After Cyber-Attack

Fig. 6 showed unemployment rates prior to and following a significant cyber-attack in five major economies: the USA, Germany, India, China, and the UK. The blue bars represent the unemployment rate prior to the attack, while the orange bars indicate a substantial rise that followed the attack. India and China experienced the most significant repercussions, with unemployment rates increasing from 6.2% to 9.0% and from 5.0% to 7.8%, respectively, primarily due to job losses in the banking, IT, and manufacturing sectors. The USA experienced a rise from 4.0% to 6.5%, signifying extensive layoffs in enterprises impacted by financial disturbances. Germany and the UK experienced an increase in unemployment, reaching 5.2% and 6.0%, respectively, which is indicative of economic downturns and diminished recruitment. This data illustrates how a significant cyber-attack can disrupt enterprises, diminish customer confidence, and compel corporations to reduce their workforce, resulting in substantial unemployment and economic instability.

How Cyber-Attack Impacts Growth Rate (Country-wise)

A country's growth rate, measured by its Gross Domestic Product (GDP), reflects its economic expansion over a specific period. Elements that facilitate this growth include industrial productivity, technical progress, investment inflows, and financial stability. Nonetheless, a substantial cyber-attack on essential sectors, particularly financial institutions, governmental infrastructure, and enterprises, can profoundly impede this advancement.

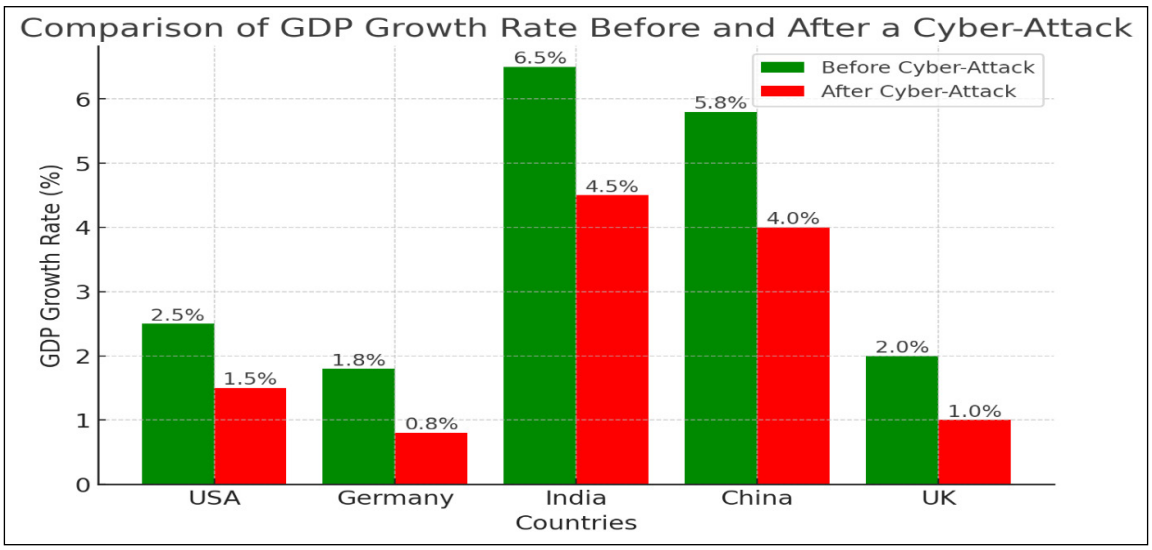

Fig. 7: Comparison of Growth Rate Country-Wise Before and After a Major Cyber-Attack

Fig. 7 compares the GDP growth rates of five major economies (the USA, Germany, India, China, and the UK) before and after a significant cyber-attack. The green bars indicate the growth rate prior to the attack, while the red bars illustrate the subsequent decline. India and China, as rapidly expanding economies, experienced elevated pre-attack growth rates of 6.5% and 5.8%, respectively. However, cyber disruptions reduced their growth rates to 4.5% and 4.0%, respectively. The United States and Germany experienced a 1% decline in GDP growth, indicating significant deceleration in both financial and industrial sectors. The UK, exhibiting a pre-attack growth rate of 2.0%, experienced a 50% reduction to 1.0%, underscoring its susceptibility to economic and business cyber risks. This comparison highlights the potential of cyber-attacks to destabilize economies, diminish investor confidence, and impede overall growth, underscoring the critical necessity for enhanced cyber-security infrastructure in digital economies.

Cyberattacks: A Threat to Consumer Trust and Financial Stability

A major cyberattack on a financial institution can severely damage consumer trust, leading to long-term reputational and economic consequences.

Fig. 8 illustrates the effects of a significant cyberattack on a financial institution by contrasting key parameters before and after the occurrence. It underscores a substantial decrease in customer trust, plummeting from 85% to 40%, and a decline in customer retention, which falls from 90% to 60%, indicating a deterioration in consumer confidence. The stock price declines from $150 to $90, indicating a

decline in investor confidence. Conversely, financial losses escalate significantly from $5 million to $300 million, highlighting the profound economic repercussions of a cyberattack. These findings underscore the crucial need for robust cyber-security protocols to protect financial institutions against reputational damage and financial instability.

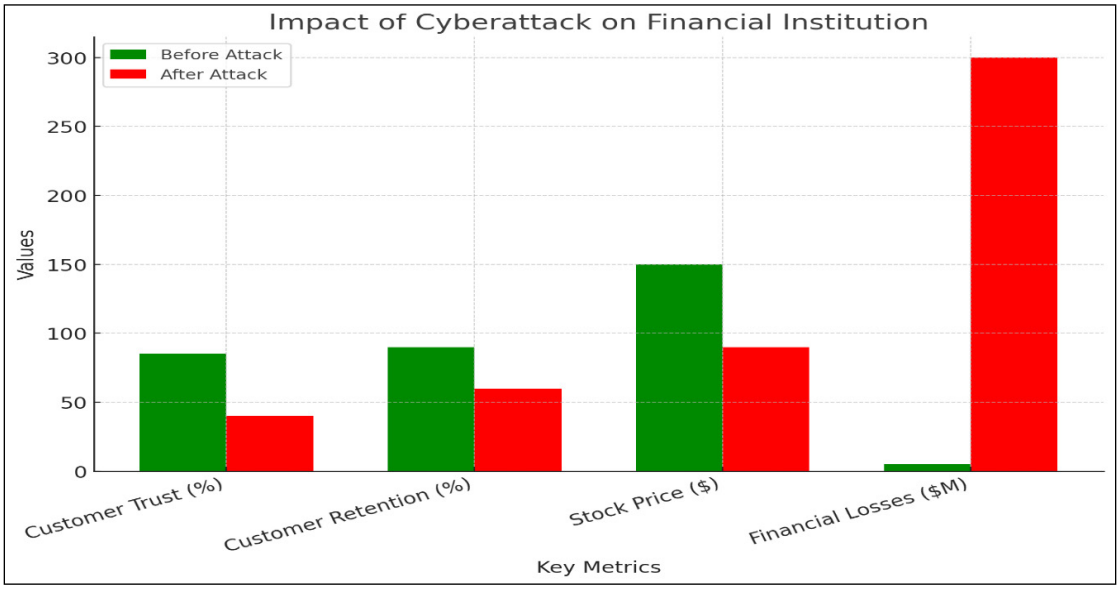

Fig. 8: Comparing key metrics before and after a major cyberattack on a financial institution

Recommendations

The rising incidence of cyber threats, such as phishing, ransomware, Distributed Denial-of-Service (DDoS) attacks, and insider threats, necessitates a comprehensive and multifaceted security approach in digital banking to safeguard customer trust and financial stability. Financial institutions must adopt a sophisticated cyber-security framework that incorporates AI-driven threat detection, blockchain technology for secure transactions, zero-trust architecture, and cloud-based encryption to reduce risks and improve resilience. The CUBE Security Model—comprising Continuous Authentication & AI Threat Detection (C), Unified Threat Intelligence & Response (U), Blockchain-Based Secure Transactions (B), and Encrypted Cloud-Based Data Protection (E)—offers a systematic framework for addressing contemporary cyber threats through the utilization of AI-driven anomaly detection, instantaneous identity verification, and dynamic security protocols to thwart unauthorized access. Moreover, quantum-resistant encryption guarantees data protection against future threats, while homomorphic encryption enables financial organizations to handle sensitive information without risking exposure to breaches. Decentralised identity verification (DID) mitigates the risks associated with centralised identity storage by facilitating self-sovereign authentication, thereby reducing the likelihood of credential theft.

Moreover, AI-powered fraud detection systems can scrutinise transaction patterns instantly, enhancing the ability to detect and prevent fraudulent activity before financial loss occurs. The integration of behavioural analytics with role-based access control (RBAC) enhances protections against insider threats by continuously monitoring user activities and restricting access to critical financial systems based on

employment roles. To mitigate extensive DDoS attacks, financial institutions can employ AI-driven traffic monitoring, web application firewalls (WAFs), and cloud-based load balancing to ensure service uptime and reduce malicious interruptions. Implementing these innovative solutions within a unified security framework can strengthen cyber-security defenses, protect customer data, ensure regulatory compliance, and bolster long-term consumer confidence, thereby safeguarding financial institutions against evolving cyber threats in a progressively digitized economy.

Limitations

During the investigation, several factors may impact the results. Includes, but not limited to:

Limited data access: Obtaining comprehensive data on cyber-security breaches, banking operations, and socio-economic repercussions is challenging. Companies may suppress crucial information to maintain consumer trust and reputation.

Cyber-security Threats: The Dynamic Nature of Cyber-security. Cyber-security is constantly evolving, with new threats and vulnerabilities emerging regularly. This makes it hard to keep the study current and relevant.

Regional and Regulatory Variances: Digital banking, cyber-security, and socio-economic conditions vary significantly across regions and countries. This variation may restrict the worldwide applicability of the findings. Measuring the socio-economic implications of cyber-security risks is complex, as it involves issues such as customer trust, economic losses, and regulatory penalties. These characteristics are hard to isolate and measure. The study may rely primarily on secondary sources, such as reports, case studies, and publically available data, which may restrict the accuracy and depth of insights compared to primary data collecting.

Limited Time and Resources: A thorough investigation may be constrained by time, finances, and expertise, which can impact its scope and depth.The study acknowledges its limits in providing a transparent view of its findings and breadth, enabling a more educated assessment of its results.

CONCLUSION

The rapid advancement of digital banking has revolutionized the financial sector, offering users unparalleled convenience and accessibility. This change has also revealed numerous cyber-security vulnerabilities for financial institutions and their clients, each of which is capable of significantly disrupting operations and compromising critical information. Data breaches, malware attacks, phishing schemes, insider threats, and vulnerabilities associated with third-party services collectively form a complex array of dangers that necessitate rapid and continuous vigilance. The socio-economic consequences of these cyber-security threats are significant and extensive. Financial losses experienced by banks and customers can lead to diminished consumer confidence, which is crucial for the stability of the economic system. Reputational harm from cyber-security issues can deter clients from using digital financial services, thereby hindering the growth of the digital economy.

Moreover, regulatory oversight and potential penalties exacerbate the operational challenges faced by financial institutions, especially smaller entities that may lack the resources to establish robust cyber-security protocols. Furthermore, the ramifications of cyber-security threats extend beyond individual and institutional spheres; they can influence broader societal dynamics, intensifying existing disparities and

presenting national security challenges. Marginalized groups frequently suffer the most from cybercrime, underscoring the necessity for comprehensive rules that protect all consumers within the digital banking framework. A comprehensive strategy is crucial for effectively mitigating these risks. This entails the implementation of sophisticated technical solutions, the augmentation of regulatory frameworks, the advancement of consumer education, and the cultivation of collaboration among industry players. By emphasizing cyber-security, financial institutions can safeguard their assets and clients while enhancing the overall resilience of the economy. This study provides an in-depth examination of cyber-security threats in digital banking and their socio-economic effects, employing a mixed-methods approach. The research assesses the multifaceted nature of cyber-security risks by integrating quantitative and qualitative insights, examining both their direct and indirect impacts on digital banking systems and their broader socio-economic implications. The results indicate that cyber-security breaches lead to financial losses, operational disruptions, diminished consumer trust, economic instability, and an exacerbation of the digital divide. The research identifies several deficiencies, including the necessity to measure the indirect costs of breaches, assess the impact of new technologies such as quantum computing, and investigate the function of public-private partnerships in enhancing cyber-security resilience. Addressing these gaps is crucial for developing a comprehensive understanding of the challenges and opportunities in securing digital banking. This paper presents strategic solutions and executable frameworks to solve these concerns, emphasizing proactive cyber-security measures, regulatory compliance, user education, and stakeholder collaboration. Utilizing modern technologies, such as artificial intelligence and blockchain, while fostering robust public-private collaborations, is a crucial strategy for strengthening cyber-security defenses. The evolution of digital banking necessitates a flexible, inclusive, and progressive strategy. By addressing current research deficiencies and employing creative solutions, the digital banking ecosystem can be fortified while promoting socio-economic development. This research lays the groundwork for ongoing investigations into emerging technologies, cost assessment methods, and collaborative initiatives aimed at developing a resilient and sustainable digital financial future.

Acknowledgments

We would like to extend our sincere appreciation to those who have assisted and advised us during the development of this research topic, “Cyber-security Risks in Digital Banking and Their Socio-Economic Impacts.” We express our profound gratitude to our academic advisors, Tanvir Hassan Zoha and Arif Mainuddin, for their invaluable insights, guidance, and support during the inception and development of this project. His expertise and constructive criticism were important in defining the scope and trajectory of this research. We express profound gratitude to the National University for supplying essential resources and fostering a supportive research environment. The availability of comprehensive literature, resources, and expert guidance greatly enhanced the quality of this job. We extend our gratitude to our peers and colleagues, whose insights and discussions have enhanced our understanding of the complex relationship between digital banking and cyber-security concerns. We recognize the contributions of industry professionals and practitioners who offered empirical insights and data that underscored the practical ramifications of cyber-security risks in the financial sector. We express our profound gratitude to all individuals who contributed, regardless of the magnitude of their involvement, to the development of this research.

REFERENCES

1. Anderson, R. 2001. *Why Information Security is Hard: An Economic Perspective.* Published in: Proceedings of the 17th Annual Computer Security Applications Conference (ACSAC). This paper examines the economic challenges of information security and offers insights into the cost-benefit analysis of cyber-security.

2. He, D., Chan, S. and Guizani, M. 2015. *Cyber-security for Industrial Control Systems: A Survey.* Published in IEEE Communications Surveys & Tutorials, this paper, though focused on industrial systems, highlights cyber-security risks relevant to digital banking infrastructures.

3. Johnson, M.E. and Goetz, E. 2007. *Embedding Information Security into the Organization.*

4. Kshetri, N. 2016. *Cyber-security for Small and Medium-Sized Businesses in Developing Economies: A Major Challenge for the Global Economy.* Published in: Crime, Law and Social Change Examines cyber-security risks in developing economies, with a focus on their socio-economic impacts.

5. Published in IEEE Security & Privacy, it Discusses how organizations can integrate cyber-security measures into their operational frameworks, especially in the financial sector.

6. Romanosky, S., Ablon, L., Kuehn, A. and Jones, T. 2019. *Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?* Published in the Journal of Cyber-security, this article offers insights into how financial institutions manage cyber-security risks through insurance, examining the economic implications.

7. Accenture, 2022. *The State of Cyber-security Resilience.* A report on how organizations are adapting to increasing cyber-security challenges and the resulting economic consequences.

8. Financial Stability Board, 2020. *Effective Practices for Cyber Incident Response and Recovery.* Discusses best practices for mitigating cyber-security risks in the financial sector, with an emphasis on socio-economic stability.

9. IBM Security, 2021. *Cost of a Data Breach Report 2021.* Provides detailed statistics and analyses on the financial impacts of data breaches in various industries, including banking.

10. McKinsey and Company, 2021. *The Future of Cyber-security in Banking.* Examines the evolving cyber-security landscape in digital banking, with insights into the socio-economic ripple effects.

11. World Economic Forum, 2022. *The Global Risks Report 2022.* Explores global cyber-security threats and their economic implications, with sections dedicated to the financial services sector.

12. NIST Cyber-security Framework, 2020. A comprehensive guide for managing and mitigating cyber-security risks, widely used in the banking industry.

13. Schneier, B. 2015. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.* This book examines the broader implications of cyber-security and data privacy, with a particular focus on their relevance to financial systems.

14. Solomon, M.G. and Chapple, M. 2018. *Information Security: Principles and Practices.* Covers foundational principles of cyber-security with applications in banking and finance.

15. Stallings, W. and Brown, L. 2021. *Computer Security: Principles and Practice.* A detailed exploration of cyber-security principles, including economic impacts and risk assessment techniques.

16. MIT Technology Review – Cyber-security Section, regularly updated articles and reports on cyber-security trends and challenges in the digital economy.

17. The Economist – Financial and Technology Sections, Analysis of the economic impacts of cyber-security threats in banking.