CYBER SECURITY CHALLENGES THROUGH CASE STUDY AND DATA PERSPECTIVE IN BANKING SECTOR

BY

ALI ASIF
ID: 213-17-494

This Report Presented in Partial Fulfillment of the Requirements for
The Degree of MS in Management Information System

Supervised By

Dr. Md Zahid Hasan
Associate Professor
Department of CSE
Daffodil International University

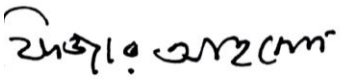
DAFFODIL INTERNATIONAL UNIVERSITY
DHAKA, BANGLADESH
May 2025

APPROVAL

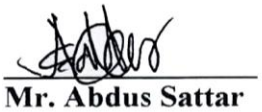
This Thesis titled "CYBER SECURITY CHALLENGES THROUGH CASE STUDY AND DATA PERSPECTIVE IN BANKING SECTOR", submitted by Ali Asif, ID: 213-17-494 and to the Department of Computer Science and Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Master of Science in Management Information System and approved as to its style and contents. The presentation has been held on 23-05-2025.

BOARD OF EXAMINERS

Dr. Sheak Rashed Haider Noori — **Board Chairman**
Professor and Head
Department of CSE
Faculty of Science & Information Technology
Daffodil International University



Dr. Fizar Ahmed — **Internal Examiner 1**
Associate Professor
Department of CSE
Faculty of Science & Information Technology
Daffodil International University



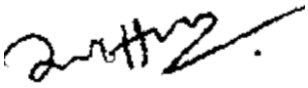
Mr. Abdus Sattar — **Internal Examiner 2**
Associate Professor
Department of CSE
Faculty of Science & Information Technology
Daffodil International University

Sadat Hasan — **External Examiner**
Data Scientist
Risk Management Division,
BRAC Bank Limited

DECLARATION

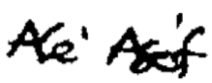
I, Ali Asif, ID: 213-17-494, hereby declare that the thesis titled **"Cyber Security Challenges through Case Study and Data Perspective in Banking Sector"** is my original work and has not been submitted elsewhere for any degree or diploma. Any references to the work of others have been clearly cited and acknowledged.

Supervised by:



Dr. Md Zahid Hasan
Associate Professor
Department of CSE
Daffodil International University

Submitted by:



Ali Asif
ID: 213-17-494

ACKNOWLEDGEMENT

I express my heartiest thanks and gratefulness to Almighty Allah for his divine blessings, which made it possible to complete my thesis successfully.

I would like to express my sincere gratitude to my supervisor, Dr. Md Zahid Hasan, Associate Professor, Department of Computer Science and Engineering, Daffodil International University, for his continuous guidance, insightful feedback, and strong encouragement throughout this research.

I also thank all the faculty members of the MIS Department at Daffodil International University who supported me during this academic journey.

Lastly, I am forever indebted to my family for their love, patience, constant support and motivation.

ABSTRACT

Management Information Systems (MIS) are crucial in today's digital banking environment, but they are also becoming more vulnerable to cybersecurity attacks. Using qualitative techniques such as expert interviews, case study analysis specifically, the 2016 Bangladesh Bank Heist and secondary data, this study investigates these issues in the context of bangladesh. The results show that vulnerabilities are caused by inadequate governance, training, and budget allocation in addition to obsolete systems and insufficient authentication. The study identifies a gap between policy and practice and suggests immplementing international standards like as ISO/IEC 27001 and the NIST Framework to increase monitoring, multi-factor authentication, and red-teaming in order to enhance MIS security.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1
INTRODUCTION

1.1 Background of the Study

The banking industry has undergone a significant transformation over the last twenty years due to the extensive use of digital technologies. Central to this change is the integration of Management Information Systems, which assist in optimizing operations, handling financial data, facilitating compliance reporting, and improving customer service delivery. As banking increasingly relies on data, the reliances on digital systems has opened up new opportunities for cyber threats.

Cybersecurity encompasses a range of tools, policies, concepts, and practices aimed at safeguarding digital systems, networks, and data from unauthorized access, attacks, damage, or theft. In the banking sector, cybersecurity is closely linked to MIS security, as these systems manage crucial financial and parsonal information, oversees transaction processes and assist in institutional decision making. Ensuring the security of MIS is essential for preserving the confidentiallity, integrity and availability of banking activities.

Management Information Systems commonly connect with outside financial networks like SWIFT and work with third party providers. While these integrations improve efficiency, they also bring considerable security threats. In nations such as Bangladesh, where banking institutions may not have modern infrastructures or established cybersecurity policies, this risk is even greater.

The merging of outdated systems, ineffective implementation of cybersecurity measures and lack of skilled personnel renders numerous banks vulnerable to attacks. A notable example is the Bangladesh Bank Heist (2016), in which intruders took advantage of endpoint vulnerabillities and breached the SWIFT system to illegally transfer $81 million from the central bank's reserve account. This event illustrates the devastating consequences of management information system weaknesses when cybersecurity protocols are lacking.

This paper invastigates these cybersecurity challenges through the real world incidents and experts analysis, focusing on how financial institutions particularly in developing countries can enhance MIS resilience by aligning with global cybersecurity standards.

1.2 Problem Statement

Despite the critical role MIS plays in banking operations, many financial institutions continue to operate with fragmented security architectures, legacy systems and underfunded IT departments. These creates exploitable weaknesses, leaving banks vulnerable to data breaches, financial fraud and operational disruptions. The Bangladesh Bank Heist exemplifies the real world implications of cyber negligence in banking IT systems. A review of the incident revealed that fundamental security controls such as firewalls, real time monitoring and endpoint protection were either absent or poorly implemented.

Furthermore, there is a significant gap between cybersecurity policy frameworks and their execution. In countries like bangladesh, regulatory oversight often lacks enforcement capacity and executive level awareness remains low. As cyber threats become more sophisticated, this gap presents an increasing risk not only to individual institutions but also to national financial stability.

1.3 Objectives of the Study

This research aims to:

- Identify key cybersecurity challenges associated with the use of MIS in the banking sector.
- Analyze real-life cases of cybersecurity failures, with an emphasis on the Bangladesh Bank Heist.
- Evaluate the current cybersecurity readiness of Bangladeshi banks.
- Recommend actionable strategies to enhance MIS security and governance in financial institutions.

1.4 Research Questions

To achieve these objectives, the study seeks to address the following questions:

I. What are the most prevalent cybersecurity threats to MIS in banks?
II. How did cybersecurity lapses contribute to the Bangladesh Bank Heist?
III. What measures are Bangladeshi banks currently taking to secure MIS?
IV. How can these measures be improved to align with global best practices?

1.5 Scope and Limitations

This study is centered on cybersecurity issues related to MIS in the banking sector, with a primary focus on banks operating within Bangladesh. While global case studies are considered to provide comparative insights, the core analysis revolves around domestic institutions. Non-banking financial institutions and fintech entities are excluded to maintain a focused scope.

The study is limited by restricted access to internal cybersecurity documentation, a common challenge due to confidentiality concerns. Moreover, some banks were reluctant to disclose full details of past security incidents, potentially limiting the depth of analysis in specific cases.

1.6 Report Layout

This thesis is organized as follows:

- **Chapter 1: Introduction** – Provides the background, problem statement, research objectives, and scope of the study, with a focus on cybersecurity issues within Management Information Systems (MIS) in the banking sector.
- **Chapter 2: Literature Review** – Summarizes existing academic and industry literature related to cybersecurity in MIS, highlighting key threats, notable case studies, and gaps in research particularly relevant to the Bangladeshi banking context.
- **Chapter 3: Methodology** – Describes the qualitative research approach, including case study analysis, expert interviews, and data collection methods. It also introduces the analytical framework used to interpret findings.
- **Chapter 4: Findings and Recommendations** – Presents the main outcomes of the research, supported by interview themes, comparative analysis, and visual data. It offers actionable recommendations to strengthen cybersecurity in banking MIS environments.
- **Chapter 5: Conclusion** – Summarizes the key findings, research contributions, and limitations of the study. It also provides suggestions for future research directions and highlights the broader implications for policy and practice in developing countries like Bangladesh.

CHAPTER 2
LITERATURE REVIEW

2.1 Introduction

Management Information System (MIS) is an integrated system that provides organizations with the tools to collect, process, store and disseminate information for effective planning, control and decision-making. MIS combines people, technology, data and business proceeses to generate timely and relevant reports that assist managers in making strategic, tactical, and operational decisions. The increasing reliance on Management Information Systems (MIS) in banking institutions has significantly improved operational efficiency, risk analysis and compliance reporting. However, this digital transformation has simultaneously introduced critical vulnerabilities that expose financial institutions to cyber threats. This literature review synthesizes current academic and industry findings related to cybersecurity in MIS within the banking sector, identifying gaps and highlighting trends relevant to developing economies like Bangladesh.

2.2 The Role of MIS in Banking Operations

Management Information Systems in banks serve as integrated frameworks for data collection, storage, processing and decision-making. Functions typically supported by MIS include customer relationship management, anti-money laundering (AML) monitoring, credit risk assessment and strategic business forecasting.

These systems frequently interact with external platforms such as SWIFT, credit bureaus and cloud-based services, creating complex digital ecosystems with increasing points of vulnerability.

2.3 Cybersecurity and its Threats

Cybersecurity refers to the practices, technologies, and processes designed to protect computer systems, networks, programs and data from unauthorized access, cyberattacks, damage or theft. It ensures the confidentiality, integrity and availability (often abbreviated as the **CIA triad**) of digital information.

Cybersecurity involves multiple layers of defense, including:

- **Technical controls** (e.g., firewalls, encryption, intrusion detection systems)
- **Administrative policies** (e.g., access control, user training, governance frameworks)
- **Operational measures** (e.g., incident response, regular patching, vulnerability scanning)

2.4 Cybersecurity in MIS

The relationship between cybersecurity and Management Information Systems (MIS) lies in the fact that MIS stores, processes, and transmits sensitive organizational data, while cybersecurity provides the necessary protection to ensure the confidentiality, integrity, and availability of that data against cyber threats. Without effective cybersecurity, MIS cannot operate securely or reliably in a digital environment.

2.5 Cybersecurity Threats in MIS

MIS infrastructure is vulnerable to a wide array of cybersecurity threats. These include:

- **Malware and Ransomware Attacks**: Widely recognized as persistent threats, ransomware campaigns such as WannaCry and NotPetya have disrupted banking operations across Asia and Europe [4], [5].
- **Phishing and Social Engineering**: Human error remains a primary attack vector, especially in institutions lacking robust employee training programs [6].

- **Insider Threats**: Insider incidents often arise due to misuse of privileged access or inadequate access control policies [7].
- **Distributed Denial-of-Service (DDoS)**: These attacks disrupt availability and can serve as distractions for more complex intrusions [8].
- **Zero-Day Exploits**: Financial institutions often struggle with patch management, making them susceptible to unknown vulnerabilities [9].

2.6 Case-Based Evidence

Several case studies underscore the severity of MIS-related cybersecurity failures:

- **Bangladesh Bank Heist (2016)**: Hackers exploited unpatched systems and poor endpoint controls to initiate unauthorized SWIFT transfers, resulting in an $81 million loss [10].
- **Target Corporation Breach (2013)**: Although not a bank, the breach via a third-party HVAC vendor illustrates the dangers of poor vendor vetting—a lesson highly applicable to banks [11].
- **JPMorgan Chase Breach (2014)**: Hackers compromised data of 76 million households and 7 million businesses by exploiting a simple security flaw, demonstrating how even advanced institutions remain at risk [12].

2.7 Cloud and Third-Party Risks

The shift toward cloud-based MIS introduces new security paradigms. Studies reveal that many banks misunderstand the shared responsibility model in cloud security, placing sensitive data at risk due to misconfigurations or poor vendor practices [13], [14].

Third-party vendors, such as those handling KYC verifications or outsourced IT functions, frequently operate outside the bank's direct control but within its digital perimeter. This dependence necessitates stringent third-party risk management frameworks [15].

2.8 Security Governance and Policy Gaps

Cybersecurity governance in banks is often reactive rather than proactive. Many institutions lack a centralized security operations center (SOC) or up-to-date incident response plans [16]. In developing countries, regulatory enforcement is weak, and banking boards often deprioritize cybersecurity due to cost concerns [17].

2.9 Literature Gaps Identified

While there is extensive literature on banking cybersecurity, most studies are either:

- Focused on **technical mechanisms** without contextualizing operational or managerial failures; or
- Geared toward **developed economies**, offering limited relevance for countries like Bangladesh where infrastructural and policy maturity is still evolving [18]–[20].

This gap necessitates more region-specific research that accounts for governance challenges, cultural dynamics, and infrastructural limitations in cyber defense strategies.

CHAPTER 3
METHODOLOGY

3.1 Research Approach

The Bangladesh Bank Heist, which occurred in February 2016, is one of the most notorious cyberattacks in banking history, involving the theft of $81 million from the central bank's account at the Federal Reserve Bank of New York. Hackers infiltrated Bangladesh Bank's internal network, likely through phishing and unpatched Windows systems, and installed malware on computers linked to the SWIFT financial messaging platform. They observed transaction behavior and used stolen credentials to send 35 fraudulent SWIFT messages attempting to transfer nearly $1 billion to accounts in the Philippines and Sri Lanka. While most transfers were blocked due to suspicious routing details, five succeeded, resulting in the loss of $81 million, most of which was laundered through Philippine casinos. The attackers masked their activities by disabling printers and erasing transaction logs, delaying detection. The breach exposed severe security flaws, including the absence of a firewall, outdated infrastructure, lack of two-factor authentication, no real time monitoring and insufficient staff awareness. This incident not only revealed vulnerabilities in the bank's MIS infrastructure but also triggered global financial institutions and SWIFT to adopt stricter cybersecurity protocols, highlighting the critical importance of securing MIS systems in the banking sector.

This study employs a qualitative case study approach, combining document analysis, expert interviews and seccondary data review. The rationale is to uncover contex-rich insights about cybersecurity challenges in MIS environments that quantitative data alone may not fully explain .

The research uses an interpretive paradigm, aiming to understand institutional vulnerabilities, behavioral patterns, and governance gaps that contribute to cyber threats in banking systems.

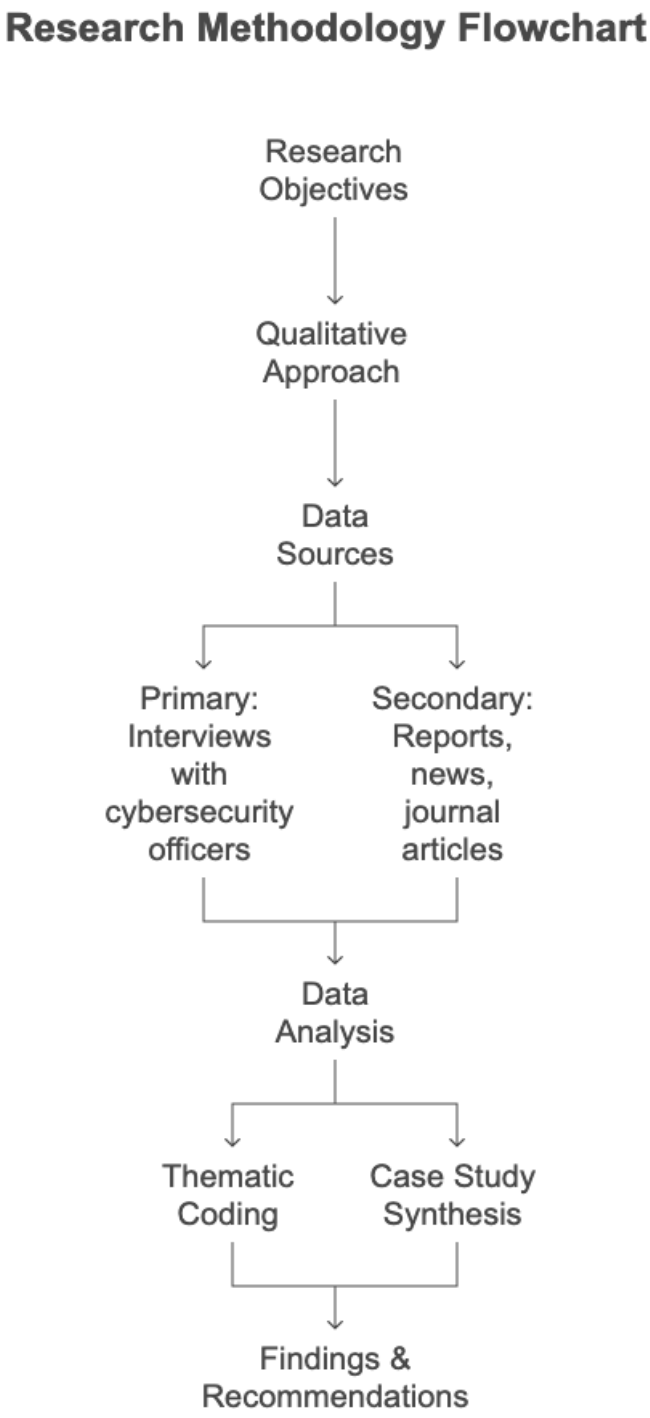


Figure 3.1: Research Methodology Flowchart

3.2 Research Design

The research is structured around the exploratory case study model with supporting comparative analysis. Figure 3.2 illustrates this multi-level framework:

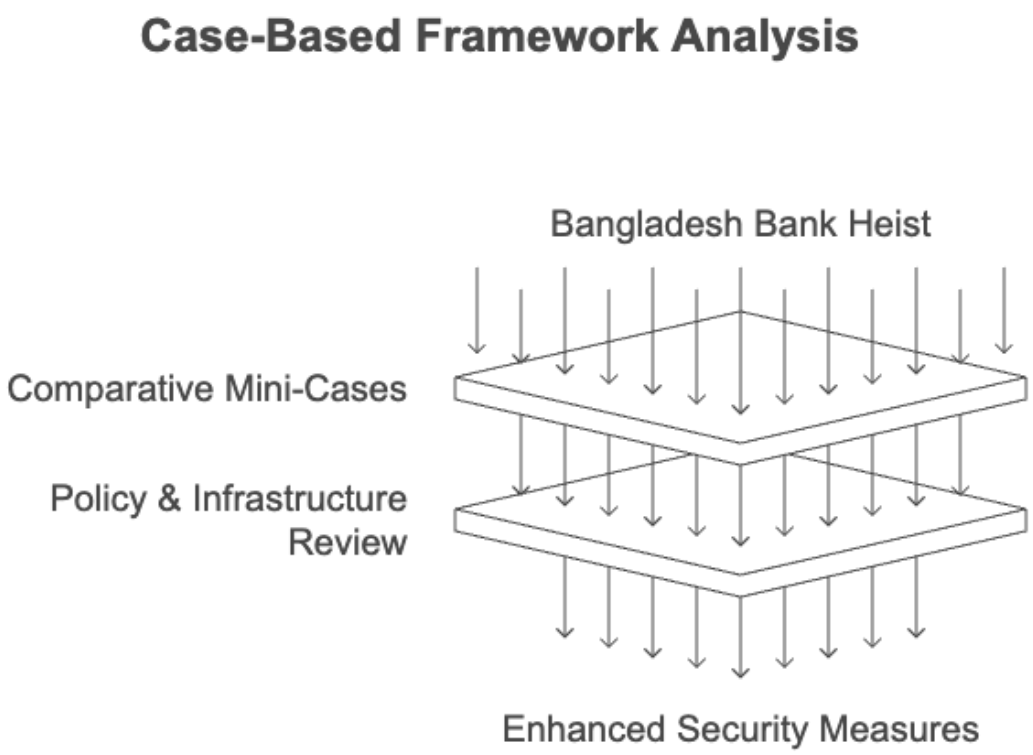


Figure 3.2: Multi-Layered Case-Based Framework

3.3 Data Collection Methods

This study utilized a multi-source qualitative data collection strategy, integrating semi-structured interviews**,** document analysis and literature synthesis. The approach was chosen to enable triangulation and contextual depth, which are essential for investigating systemic cybersecurity challenges within Management Information Systems (MIS) in the banking sector.

3.3.1 Semi-Structured Interviews

Primary data was collected through semi-structured interviews with three professionals currently serving in the cybersecurity or IT governance departments of commercial banks in Bangladesh. The interviews aimed to capture lived experiences and expert interpretations of cybersecurity practices, gaps, and regulatory compliance challenges within MIS environments.

Interview participants were selected via purposive sampling, targeting individuals who:

- Have more than five years of experience in banking IT or cybersecurity
- Hold decision-making or implementation roles (e.g., Security Officer, MIS Officer)
- Represent institutions operating under the supervision of Bangladeshi Banks

Each interview lasted between **10 to 15 minutes**, conducted in-person. Conversations were guided by a pre-approved interview protocol, and all participants consented to be interviewed anonymously.

Sample Interview Questions and Answers Included:

I. Q: What are the most pressing cybersecurity risks your bank currently faces?

   A: The most critical cybersecurity risks are poor endpoint protection, lack of network segmentation, and the absence of real-time monitoring systems. Attackers exploited these weaknesses to infiltrate the internal systems and manipulate SWIFT transactions without detection.

II. Q: How often are security policies updated, and who is responsible for enforcement?

   A: Cybersecurity policies are either outdated or inadequately enforced. There is no centralized authority like a dedicated CISO or formal incident response team. Policy enforcement was reactive with no evidence of routine audits, revisions or testing for vulnerabilities.

III. Q: What is the current state of your MIS infrastructure (patching, segmentation, redundancy)?

A: MIS infrastructure is partially modernized. Core systems are updated regularly, but many peripheral services still run on outdated platforms. Patching is scheduled quarterly but often delayed due to operational dependencies. Network segmentation exists but is minimal, and redundancy planning is limited to backup servers without real-time failover capability.

IV. Q: Are there regular employee training or phishing simulation programs?

A: There was a severe lack of cybersecurity awareness among staff. Employees were not trained to recognize phishing attempts or unauthorized system activity. After the attack, Cybersecurity awareness training is conducted annually. However, it is often theoretical with little interactivity. Phishing simulations are rare or nonexistent, and employees often struggle to identify social engineering threats. There is a need for ongoing, scenario-based training with measurable outcomes.

V. Q: What challenges do you face in securing third-party integrations (e.g., SWIFT, cloud vendors)?

A: Third-party security assessments are not standardized. Vendors often lack cybersecurity certifications (e.g., ISO 27001), and the bank has limited visibility into their security practices. With platforms like SWIFT, compliance with mandatory controls exists on paper, but gaps remain in local implementation and endpoint monitoring.

VI. Q: How is the cybersecurity budget allocated, and does it meet your operational needs?

A: Cybersecurity budget allocation is below 2% of the total IT budget, which is significantly lower than international benchmarks. Most of the budget goes toward compliance documentation, antivirus software, and licensing. Strategic investments in threat intelligence, advanced monitoring, and employee development are often deprioritized due to budget constraints.

Interview questions were open-ended, allowing flexibility for elaboration while maintaining thematic coherence across responses. Transcripts were anonymized to preserve institutional and individual confidentiality.

3.3.2 Document and Policy Review

Secondary data sources included:

- Public cybersecurity audit summaries from central and commercial banks
- The Bangladesh Bank Annual Financial Stability Reports (2020–2023)
- Incident response disclosures and international case reports (e.g., SWIFT CSP advisories)
- Academic and industry whitepapers published by NIST, ISACA, and ISO

These documents were reviewed to supplement and triangulate interview findings, offering an institutional and regulatory perspective on cybersecurity readiness.

3.3.3 Ethical Considerations

All interviews were conducted under informal consent agreements, and participants were informed of the study's academic purpose. No identifying information—such as bank name or personal identifiers—was not included in the report. Data was stored securely, and only aggregate themes were used in analysis.

The combination of practitioner insight and documentary evidence provided a balanced understanding of the cybersecurity landscape in Bangladeshi banks, forming the empirical backbone of this research.

3.4 Sampling Strategy

The primary data includes purposive sampling, targeting professionals with direct exposure to cybersecurity operations within commercial banks. The interview participants were chosen based on:

- Years of experience in cybersecurity or MIS
- Access to or involvement in institutional policy-making
- Availability and consent for semi-structured interviews

3.5 Thematic Analysis

Collected qualitative data was coded manually and categorized into themes aligned with the research questions. Themes included:

- Organizational awareness
- Infrastructure limitations
- Policy enforcement
- Employee behavior and training
- External integration risks

These themes were then mapped against real-world incidents to identify patterns, which are discussed further in Chapter 4.

3.6 Case Study Overview

The Bangladesh Bank Heist, which occurred in February 2016, is one of the most prominent cyberattacks targeting a central financial institution. Cybercriminals made an effort to move $951 million from the Bangladesh Bank's account at the Federal Reserve Bank of New York, successfully stealing $81 million, which was subsequently laundered through casinos in the Philippines. This event underscores significant cybersecurity deficiencies with the MIS infrastructure, such as endpoint vulnerabilities, inadequate authentication and the absence of real-time monitoring.

3.7 Attack Lifecycle

The assailants employed a multi-layered strategy, utilizing malware, credential theft, and manipulation of SWIFT systems. The breach at Bangladesh Bank unfolded through a meticulously coordinated process, starting with the initial infiltration of internal networks via malware insertion, likely executed through phishing attacks or USB devices. Subsequently, the attackers engaged in credential theft by observing user behavior and capturing login information for SWIFT messaging platforms. During the execution of the attack, they generated fake SWIFT messages to authorize illicit fund transfers. To evade prompt detection, they employed tactics such as disabling printers and erasing logs. The concluding phase involved money laundering, where the misappropriate funds were channeled through intarmediary banks and eventually funneled into casinos located in the Philippines. This sequence of events illustrates a classic example of how operational vulnerabilities in Management Information Systems (MIS) can be exploited especially the absence of real time monitoring, segmentation and authentication layers, can be exploited to bypass traditional banking security controls. This is illustrated in **Figure 3.3**.

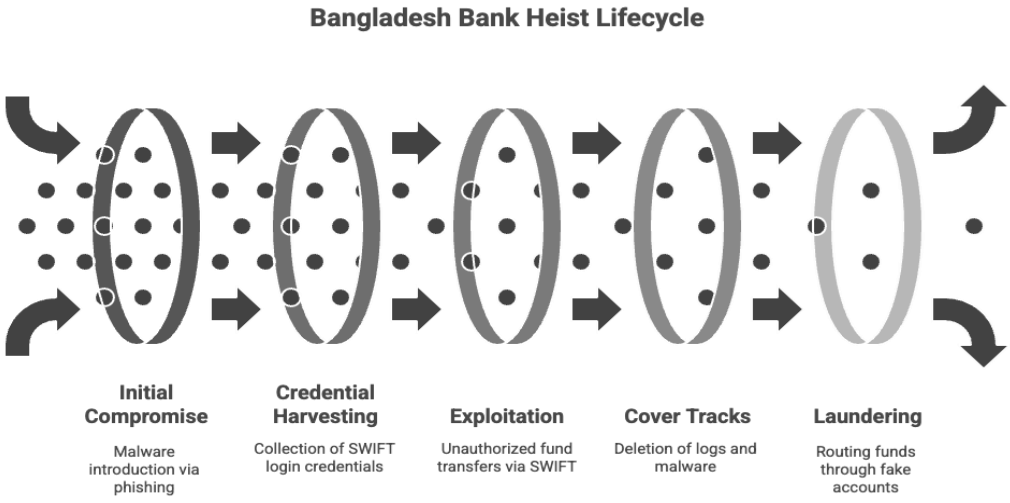


Figure 3.3: Technical Lifecycle of the Bangladesh Bank Heist

This diagram showcasing the sequential steps of the 2016 Bangladesh Bank Heist, highlighting each technical and strategic steps taken by the attackers from initial step to money laundering.

3.8 Table of Security Failures

The Bangladesh Bank Heist exposed critical security failures across six core layers of the bank's cybersecurity framework. At the network level, the absence of a firewall on the SWIFT server left the system exposed to external threats. Unpatched and outdated endpoint systems, particularly those running Windows XP, created known vulnerabilities. The lack of multi-factor authentication allowed attackers to access SWIFT terminals using only stolen credentials. Additionally, the absence of real time monitoring systems such as SIEM delayed breech detection. Weak IT governance and insufficient audit mechanisms further hindered incident escelation, while untrained employees failed to recognize early signs of intrusion. Together, these failures reflect a systemic breakdown in MIS-related cybersecurity practices.

Layer	Failure Point	Details
Network Security	No firewall on SWIFT server	Open network perimeter
Endpoint Security	Unpatched Windows XP systems	End-of-life OS with known vulnerabilities
Authentication	No multi-factor authentication (MFA)	Login via username/password only
Monitoring	No real-time alerts or SIEM	Breach detection delayed
Governance	Poor internal IT governance	No audit trail or escalation mechanisms
Employee Training	Lack of cybersecurity awareness	Employees unaware of breach indicators

Table 3.1: Multilayered Security Failures in the Bangladesh Bank Heist

This table presents the key cybersecurity weaknesses exploited in the 2016 Bangladesh Bank Heist, categorized by security layer, failure point, and technical impact.

3.9 Lessons from the Case Study

The Bangladesh Bank Heist underscores a pattern of systemic failure. The incident is not solely a technological lapse, but also a **failure in policy, training, and governance**. It aligns directly with the themes extracted from interviews and literature:

Theme	Insight from Case Study
Organizational Awareness	Executive board unaware of endpoint risk
Infrastructure Deficiencies	Legacy systems with no updates
Policy Enforcement	No mandatory security policies for privileged access
Human Factors	No red-team exercises, weak employee training
Integration Risk	SWIFT trusted blindly without risk checks

Table 3.2: Lessons from the Bangladesh Bank Heist Mapped to Cybersecurity

This table links the thematic findings of the case study to specific institutional failures, emphasizing that the heist resulted not just from technical lapses but also from broader issues in policy enforcement, awareness, and governance. As it encapsulates the interplay between outdated MIS infrastructure, poor governance, and high-impact cybersecurity threats in developing nations.

3.10 Data Collection Techniques

This study utilized a multi-source qualitative design:

Instrument	Purpose	Format
Semi-structured interviews	Gather in-depth practitioner insights	Audio-transcribed text
Document analysis	Extract themes from reports & policies	Textual & tabular
Case study synthesis	Identify structural/systemic vulnerabilities	Thematic case analysis

Table 3.3: Data Collection Instruments Used in the Study

This table outlines the qualitative tools employed in the research, detailing the purpose and format of each method, including interviews, document analysis, and case study synthesis.

3.11 Analytical Frameworks Used

The following analytical and compliance frameworks were used to interpret and validate findings:

Framework	Purpose in Study
NIST Cybersecurity Framework (CSF)	Benchmarking banks' practices
ISO/IEC 27001	Evaluation of MIS security controls
Thematic Coding	Identification of interview themes
SWOT Analysis	Assessing institutional readiness

Table 3.4: Analytical Frameworks Used in the Study

This table presents the key analytical models and standards applied in the research to evaluate cybersecurity posture, structure qualitative data and assess institutional readiness within banking MIS environments.

3.12 Thematic Coding & Results

The transcripts of the interviews were examinned through manual open coding, subsequently followed by axial coding to categorize the findings into overarching themes. Five primary themes emerged.

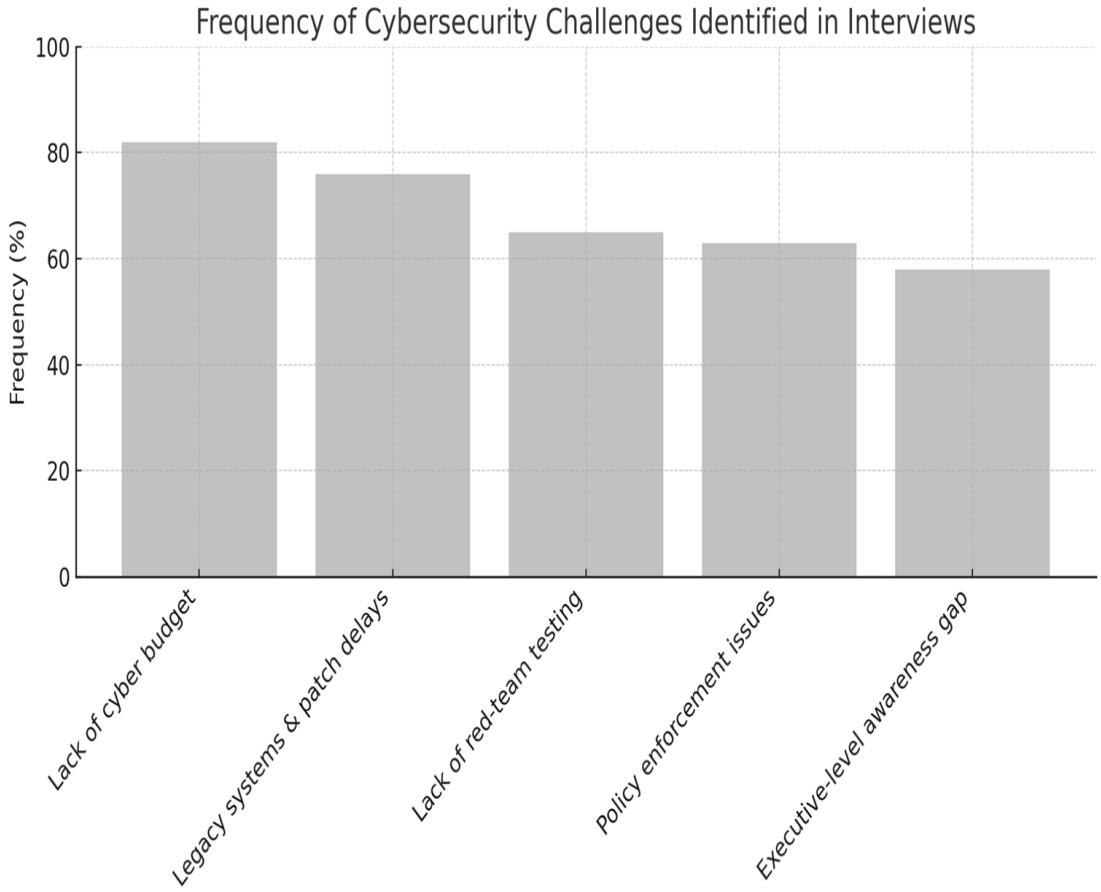


Figure 3.4: Frequency of Thematic Mentions from Interviews

The graph identified cybersecurity challenges based on frequent interviews with experts.

3.13 Table of Interview Themes and MIS Impact

Theme	Observed Impact on MIS Security	Bank Officer Quote (Paraphrased)
Budget Constraints	Delayed upgrades, minimal investment in DLP or SIEM	"Cyber isn't prioritized until an incident occurs."
Legacy Infrastructure	Insecure endpoints, frequent patching issues	"We're still running systems beyond end-of-life."
Lack of Testing	Unknown vulnerabilities persist	"We've never run a red-team simulation."
Weak Governance	Poor enforcement of access control and audit trails	"Our policies exist on paper, not in practice."
Awareness Gaps	Inconsistent cyber hygiene among staff	"People click suspicious emails without thinking."

Table 3.5: Interview Themes and Their Observed Impact on MIS Security

Insights from cybersecurity themes such as budget limitations and governance issues to their practical effects on MIS security in Bangladeshi banks.

3.14 Visualization: Risk Mapping via SWOT

The SWOT analysis indicates a varied state of cybersecurity readiness within Bangladeshi banks. Among the strengths, there is a noticeable enhancement in regulatory oversight, especially following prominent breaches like the Bangladesh Bank Heist. Additionally, banks have made in implementing core banking systems and benefiting from an expanding pool of technically proficient junior IT personnel. Nevertheless, these strengths are offset by considerable weaknesses, such as ongoing dependence on outdated infrastructure, the absence of formalized incident response teams, and inadequate training for staff in cybersecurity best practices. There are opportunities to align with international standards, including ISO/IEC and the NIST Cybersecurity Framework, as well as to take advantage of global initiatives like SWIFT's improved security protocols. However, banks also confronted with threats,

particullarly from advanced persistent threats (APTs), insider misuse and vulnerabilities introduced through third-party vendors. These results highlights the urgent necessity for banks in Bangladesh to transition from reactive compliance to proactive cybersecurity governance. Presented below is a synthesized SWOT analysis of the cybersecurity in MIS within Bangladeshi banks:

Strengths	**Weaknesses**
Increasing regulatory attention	Outdated systems still in use
Skilled junior IT professionals	Lack of formal incident response teams
Adoption of core banking systems	Weak employee awareness/training programs
Opportunities	**Threats**
International cooperation (SWIFT security)	Advanced persistent threats (APTs)
ISO/NIST standard adoption	Insider threats & third-party breaches

Table 3.6: SWOT Analysis of Cybersecurity in MIS

This table presents SWOT analysis of MIS related cybersecurity in Bangladesh's banking.

3.15 Study Limitations

The research encountered various limitations that influenced the scope and depth of its conclusions.

First, because of the confidential nature of banking operations, access to comprehensive internal cybersecurity records was limited. Secondly, the sample size was relatively small, confined to three commercial banks, as numerous institutions were reluctant to engage due to concerns regarding reputation and regulation. Additionally, there was a potential for response bias, as interviewees might have offered cautious or generalized responses to prevent revealing institutional vulnerabilities. Finally, the study was devoid of quantitative validation, such as statistical breach frequency or cost data, mainly due to the legal non-disclosure agreements (NDAs) and data protection policies that were in effect.

Limitation	Explanation
Restricted Access to Data	Confidential nature of banking operations limited full disclosure
Small Sample Size	Only three banks participated due to time and sensitivity constraints
Response Bias	Some responses may be cautious or generalized to avoid institutional exposure
Absence of Quantitative Validation	No numerical breach data due to NDAs and data protection concerns

Table 3.7: Research Limitations of the study

The main limittations of the study are listed in this table, including those pertainning to participant coverage, data availability, response bias, and the lack of quantitative breach data.

CHAPTER 4
FINDINGS AND RECOMMENDATIONS

4.1 Key Findings and Overview

The primary study findings from the Bangladesh Bank Heist and related cases are presented in this chapter, together with thematic patterns, insights from interviews, and institutional analysis. On the basis of this, technological and strategic suggestions are put forth to enhance cybersecurity in banking industry MIS environments. Many Bangladeshi banks are becoming more susceptible to sophisticated assaults as a result of the rapid evolution of cyber threats, which is outpacing their level of cybersecurity maturity. The 2016 Bangladesh Bank Heist served as an example of how extensive financial fraud can result from antiquated systems, insufficient oversight, and lax internal controls. Expert interview insights showed that cybersecurity is still not given enough attention in terms of budget allocation, with less than 2% of IT spending going towards security, which is far less than what is required by international standards. Additionally, thematic analysis uncovered systemic gaps in employee training, inconsistent policy enforcement and inadequate oversight of third-party vendors, all of which contribute to a fragille cybersecurity posture across the sector.

4.2 Common Institutional Weaknesses Identified

The analysis found a number of persistant cybersecurity flaws in organisational procedures as well as technical systems. Many banks' technical infrastructure is still based on antiquated operating systems like Windows XP and lacks adequate network segmentation, making them more susceptible to outside threats. Another significant gap was human factors, which included a lack of organised defence against social engineering and inadequate staff knowledge. Cybersecurity regulations were not consistently enforcced at the governance level, and they were frequently reactive rather than preventive. With the majority of institutions without automated alerting capabillities and real time Security Information and Event Management (SIEM) systems, the monitoring and response mechanisms were woefully inadequate. Lastly, there were frequently no formal screening procedures for third-party service providers or cybersecurity provisions in contracts, which left vendor risk unresolved.

Category	Weakness
Technical Infrastructure	Use of legacy OS (e.g., Windows XP), no network segmentation
Human Factors	Low cyber awareness, lack of social engineering defense
Governance	Weak enforcement of existing policies
Monitoring & Response	Absence of real-time SIEM and alerting tools
Vendor Risk	No cybersecurity vetting or contractual enforcement

Table 4.1: Common Cybersecurity Weaknesses Identified in Bangladeshi Banks

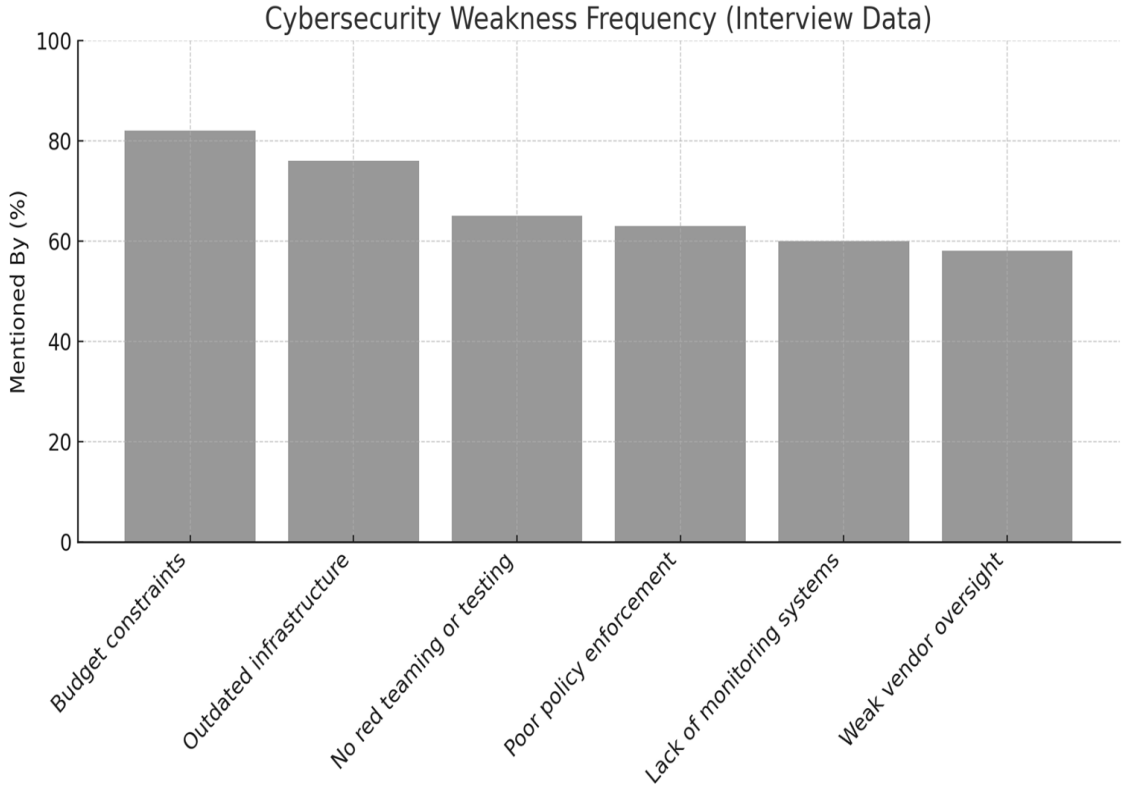


Figure 4.1: Cybersecurity Weakness Frequency (Interview Data)

4.3 Interview Insights

Interviews revealed a consistent concern regarding institutional inertia and reactive security postures. Notable statements:

- *"We wait for incidents before investing — there's no preventive budget."* (Officer A)
- *"Our systems are connected to vendors, but we don't audit them."* (Officer C)
- *"Cyber training is once a year, and most people forget it in a week."* (Officer B)

This confirms a significant disconnect between cybersecurity policy design and operational enforcement.

4.4 Comparative Budget Analysis

cybersecurity investment between Bangladesh and other regions. While banks in the United States and Western Europe allocate between **10–16%** of their IT budgets to cybersecurity, Bangladeshi banks invest **less than 2%** on average. Even Southeast Asia, as a regional peer group, spends notably more. This underfunding reflects a systemic issue in Bangladesh's cybersecurity readiness and reinforces the need for regulatory mandates and institutional prioritization of cyber defense spending.

Banking Region	% of IT Budget Allocated to Cybersecurity
United States	10–15%
Western Europe	12–16%
Southeast Asia (avg.)	8–10%
Bangladesh (avg.)	**< 2%**

Table 4.2: Comparative Cybersecurity Budget Allocation by Region

Source: ISACA State of Cybersecurity Report [16], Local bank interviews

4.5 Recommendations

Based on findings, the following recommendations are proposed:

4.5.1 Implement Stronger Authentication

- **Multi-factor authentication (MFA)** for all critical access points
- **Hardware-based tokens** for SWIFT access

System	Recommendation
Core Banking	Enforce biometric/MFA
Remote Access	VPN + Hardware Tokens
SWIFT	Smartcards/Hard tokens

Table 4.3: Authentication Enhancement Across Banking Systems

The table highlights targeted authentication upgrades—biometric/MFA for core systems, VPN with tokens for remote access, and hardware tokens for SWIFT to prevent unauthorized access and enhance system integrity.

4.5.2 Establish Mandatory Cybersecurity Training Programs

- **Annual employee training** with measurable assessments
- **Phishing simulation exercises** every quarter
- **Gamified cyber hygiene tools** to improve retention

4.5.3 Adopt Real-time Monitoring and SIEM

- Invest in **Security Information and Event Management (SIEM)** tools
- Deploy **behavioral analytics** and **anomaly detection**
- Link systems to **centralized Security Operations Centers (SOCs)**

4.5.4 Conduct Regular Penetration Testing

- Engage **ethical hackers/red teams**
- Perform **quarterly internal audits**
- Evaluate both internal systems and vendor platforms

4.5.5 Upgrade Legacy Infrastructure

To mitigate risk, banks should replace outdated systems like Windows XP, restructure flat networks using VLANs, and adopt email authentication protocols such as SPF, DKIM, and DMARC to improve threat prevention and system integrity.

Legacy Element	Upgrade Recommendation
Windows XP systems	Upgrade to Windows 11 LTS
Flat networks	Introduce VLAN-based segmentation
Email systems	Implement SPF/DKIM/DMARC filtering

Table 4.4: Recommended Upgrades for Legacy Banking Infrastructure

4.5.6 Formalize Third-party Cybersecurity Vetting

Immediate high-impact actions like MFA and monitoring tools should be prioritized, while vendor audditing and policy updates follow as medium-urgency items. The matrix helps banks allocate resourcess effectively to mitigate cybersecurity risks.

Urgency \ Impact	High Impact	Medium Impact
High Urgency	MFA, Monitoring Tools	Employee Training
Medium Urgency	Vendor Auditing	Policy Enforcement Updates

Table 4.5: Priority Matrix for Recommendation Implementation

4.5.7 Policy-Level Recommendations

Key policy intervantions include enforcing cybersecurity mandates under national law, mandating a minimum cybersecurity budget via central bank regulation and establishing internal cybersecurity governance boards within banks. These measures aim to institutionalize security and ensure long term resillience.

Policy Layer	Proposed Action
National Cyber Law	Enforce banking-specific cybersecurity mandates
Central Bank Regulation	Require minimum budget % allocation to cyber defenses
Institutional Policy Review	Create an internal Cybersecurity Governance Board

Table 4.6: Policy-Level Recommendations for Strengthening Cybersecurity Governance

CHAPTER 5
CONCLUSION

5.1 Conclusion

Cybersecurity has become an essential requirement for the banking industry rather than an optional consideration. As indicated by this study, banks in developing nations such as Bangladesh are increasingly at risk because of antiquated MIS systems and inadequate security measures. By investing wisely, implementing governance reforms, and enhancing awareness, these weaknesses can be addressed. The Bangladesh Bank Heist serves as both a warning and a motivation for institutions to align their security measures with global standards to maintain public confidence and ensure financial stability.

5.2 Limitations of the Study

The research encountered various limitations that could influence the scope of its conclusions. Access to internal data on cybersecurity incidents was limited due to the sensitive nature of banking operations, which constrained the extent of empirical validation. Furthermore, the study restricting the applicability of the findings to non-banking financial entities or different geographical areas. The number of interviews carried out was also restricted since operational limitations and participant availability impeded wider data collection.

5.3 Recommendations for Future Research

Future studies ought to incorporate quantitative research to assess the frequency of cyber breaches, the costs they incur, and the risk levels associated with various systems in Bangladeshi banks. It should also examine non-banking financial institutions (NBFIs) and emerging fintech platforms to gain a comprehensive understanding of cybersecurity throughout the entire financial sector. Furthermore, investigating how technologies such as artificial AI and machine learning can assist in the real-time detection of threats would be beneficial for enhancing the security of MIS systems.

References

[1] A. Laudon and J. Laudon, *Management Information Systems: Managing the Digital Firm*, 15th ed. Pearson, 2018.

[2] R. G. Raj and C. C. Goh, “Information systems in banking: Evolution and risk perspectives,” *Journal of Banking and Finance*, vol. 45, pp. 74–85, 2015.

[3] S. S. Amin et al., “Secure interbank communications using SWIFT: Lessons from Bangladesh,” *Information Security Journal: A Global Perspective*, vol. 28, no. 2, pp. 65–76, 2019.

[4] Symantec, “Internet Security Threat Report,” vol. 24, 2019. [Online]. Available: https://symantec.com

[5] Europol, “Internet Organized Crime Threat Assessment (IOCTA) 2022,” The Hague, 2022.

[6] Verizon, “Data Breach Investigations Report,” 2023. [Online]. Available: https://verizon.com/dbir/

[7] D. Cappelli et al., *The CERT Guide to Insider Threats*. Addison-Wesley, 2012.

[8] Cloudflare, “Understanding DDoS Attacks,” 2023. [Online]. Available: https://cloudflare.com/learning/

[9] M. Sabett and D. Bishop, “The 0-Day Dilemma: Cyber Risk and Patch Management,” *ISACA Journal*, vol. 4, pp. 34–40, 2020.

[10] S. M. Kaiser, “The Bangladesh Bank Heist and SWIFT Security Issues,” *Journal of Financial Crime*, vol. 25, no. 1, pp. 2–10, 2018.

[11] B. Krebs, *Spam Nation: The Inside Story of Organized Cybercrime*, Sourcebooks, 2014.

[12] K. Zetter, “Inside the JPMorgan Chase Data Breach,” *Wired*, Oct. 2014. [Online]. Available: https://wired.com

[13] NIST, “Framework for Improving Critical Infrastructure Cybersecurity,” Version 1.1, Apr. 2018.

[14] Gartner, “Top Risks in Cloud Computing for Financial Services,” 2022. [Online]. Available: https://gartner.com

[15] B. Schneier, “Supply Chain Security: A Growing Challenge,” *IEEE Security & Privacy*, vol. 18, no. 3, pp. 84–86, May–Jun. 2020.

[16] ISACA, “State of Cybersecurity 2023,” Global Survey Report.

[17] M. Hossain and T. M. Rahman, “Cybersecurity Readiness in Bangladeshi Banks: Challenges and Solutions,” *International Journal of Information Management*, vol. 58, 2021.

[18] M. D. Wirtz, “Cybersecurity Governance in Banking,” *Banking Technology Today*, vol. 34, pp. 19–25, 2020.

[19] A. Alasmary and H. Alhaidari, “Cybersecurity Challenges in Developing Countries,” in *Proc. of ICICIS 2021*, IEEE, pp. 85–92.

[20] S. R. Hasan, “Digital Vulnerabilities in South Asian Financial Institutions,” *Asian Journal of Information Security*, vol. 6, no. 2, pp. 44–59, 2022.