

Article

Institutional Fragility and Cross-Border Cyber Risk in Financial Systems: Insights from the 2016 Bangladesh Bank Heist

M. Sirajul Islam ^{1,2} 

¹ Department of Operations and Project Management, College of Business, Alfaisal University, Riyadh 11533, Saudi Arabia; sislam@alfaisal.edu

² Department of Informatics, Örebro University, 70182 Örebro, Sweden; sirajul.islam@oru.se

Abstract

This paper investigates how institutional fragilities shape cross-border cyber risk in financial systems, using the 2016 Bangladesh Bank heist as an illustrative case from a developing-country context. Drawing on a scoping review of the multidisciplinary literature on cybersecurity governance, financial cybercrime, and cross-border cyber risk, combined with an exploratory case study, the Bangladesh Bank heist is explored through a multi-level analytical lens encompassing macro-level institutional and geopolitical factors, meso-level ecosystem interdependencies, and micro-level organizational vulnerabilities. The analysis suggests that the 2016 heist was not solely a technical intrusion but was also associated with broader governance, regulatory, infrastructural, and organizational weaknesses. Fragmented governance arrangements, digital dependencies, limited operational resilience, inadequate cybersecurity controls, and human-factor vulnerabilities emerged as important dimensions of risk. Comparison with selected incidents from other developing and emerging economies indicates that similar patterns may occur across different institutional settings, although their manifestation remains context dependent. Rather than advancing a general theory, the highlights the importance of strengthening governance capacity, regulatory coordination, and cyber resilience within globally interconnected financial systems.

Keywords: cybersecurity; developing countries; Bangladesh Bank heist; cross-border risks; cybersecurity governance; institutional fragility; financial cybercrime

1. Introduction

When a single typo in a payment instruction nearly cost hundreds of millions of dollars, the world witnessed one of the most audacious cyberattacks in financial history and a stark alarm on the fragility of global financial security. The 2016 Bangladesh Bank heist, in which US \$81 million was siphoned via the SWIFT (Society for Worldwide Interbank Financial Telecommunication) network—a global alliance for standard financial messaging used by over 11,000 institutions, exposed a layered cross-border criminal ecosystem where sophisticated malware, fragmented governance structures and weak institutional preparedness converged [1–3]. As Adelman et al. [4] observe, it stands out not only as a major technical intrusion but as a revealing moment for developing-country exposures. What matters most is not simply the loss, but how the event exposed coordinated operations of human actors and non-human actors [1,5]. Despite numerous technical investigations and policy reports, academic understanding remains limited about how such ecosystems func-



Academic Editor: Leandros Maglaras

Received: 25 April 2026

Revised: 22 June 2026

Accepted: 26 June 2026

Published: 7 July 2026

Copyright: © 2026 by the author.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

tion across borders, how human-technological interactions unfold, and how institutional vulnerabilities, especially in developing country-contexts shape exposure [6–9].

Cybercriminal ecosystems operate at the nexus of human agents (hackers, insiders, intermediaries) and technological elements (malware, financial platforms, regulatory gaps), crossing jurisdictions and evading fragmented enforcement regimes [10–13]. Cybercriminal entities such as the North Korean government sponsored the ‘Lazarus Group’, implicated in the Bangladesh Bank attack, exemplify this global coordination, exploiting legal, technological and institutional asymmetries across borders [3,14]. In developing economies, these threats are amplified by legacy infrastructures, weak governance, immature cybersecurity protocols and partial adoption of global financial-messaging safeguards like SWIFT’s Customer Security Programme [14–16]. Existing scholarship examined technical components such as malware and advanced persistent threats [17], and explored how cyberattacks are coordinated globally [18]. Yet much of this work is rooted in the Global North or isolated to technical analyses, rarely integrating how human-technical interplay and institutional fragility converge to create the conditions for large-scale financial cybercrime [15,19]. Within this ecosystem, SWIFT itself serves as a central non-human actor, shaping how financial messages flow globally and how their interception or manipulation becomes possible when local installations are weak [20,21].

In this study, institutional fragility refers to weaknesses in the capacity of formal and informal institutions to effectively coordinate, regulate, monitor, and enforce actions necessary to manage collective risks [22,23]. Such weaknesses may manifest through fragmented governance structures, inadequate regulatory oversight, limited organizational capabilities, weak enforcement mechanisms, and insufficient inter-organizational coordination [24]. From a governance perspective, institutional fragility also reflects limitations in state and organizational capacity to formulate, implement, and sustain effective policies and oversight mechanisms [25]. Within the cybersecurity domain, these weaknesses can reduce the ability of institutions to anticipate, prevent, respond to, and recover from cyber incidents, thereby increasing systemic vulnerability to complex and transnational cyber threats. Within the cybersecurity domain, institutional fragility extends beyond technical vulnerabilities and encompasses governance, regulatory, organizational, and human factors that shape how cyber risks are identified, managed, and mitigated [26]. Emerging research increasingly recognizes that cyber resilience depends not only on technological safeguards but also on institutional capacity, effective governance arrangements, regulatory coherence, and cross-organizational coordination [16,27]. This perspective is particularly relevant in developing-country contexts, where institutional constraints may amplify the impact of cross-border cyber threats, weaken incident response capabilities, and complicate coordinated responses to cyber incidents. Accordingly, the Bangladesh Bank cyber heist is examined not merely as a technological failure, but as a manifestation of broader institutional weaknesses that shaped the bank’s vulnerability to a sophisticated transnational cyberattack.

Building on this perspective, contemporary socio-technical frameworks emphasise the interplay of people, systems and institutions in shaping cyber vulnerability [26]. Theoretical frameworks such as the Diamond Model map adversary capabilities, infrastructure and victim profiles to explain how attacks unfold [10]. While such models are useful for understanding attack mechanics and threat attribution, the present study adopts a broader socio-technical and institutional perspective that extends beyond attacker-centric analysis. Accordingly, the study focuses on the governance, regulatory, organizational, infrastructural, and human dimensions of cyber risk identified through the scoping review and examined through the Bangladesh Bank case. Such perspectives reveal that vulnerabilities are not simply technical; they emerge from co-production across human, machine and

institutional layers, especially where governance is fragmented and cybersecurity maturity is low. Consequently, cyber-resilience in financial institutions has become a strategic imperative, encompassing not just operational safeguards, but macro-level governance, board oversight and transparent disclosures [16,27]. The Bangladesh Bank case underscored organisational shortcomings including weak duty segregation, legacy configurations and the absence of formal incident-response systems. Taken together, these conditions illustrate how cyber incidents emerge not solely from technical vulnerabilities but from the interaction of technological, organizational, and institutional factors operating across multiple levels of the financial ecosystem.

Against this background, this study explores the cross-border cyber risk exposure in a developing country context and seeks to answer the core research question: *How do cross-border cyber risks exploit governance gaps and infrastructural weaknesses to enable financial cyberattacks in developing economies?* Using a socio-technical risk framework [26], it investigates the interconnected dynamics of technological fragility, human coordination and institutional fragility [5,16]. Importantly, while key research has focused on Global North settings, the developing-country context remains understudied. Institutions in such settings face distinct structural, regulatory and technological features such as limited resources, weaker rule of law and greater dependency on external systems that heighten cyber risk [15,28]. The Bangladesh Bank heist thus becomes a paradigmatic example of how sophisticated actors exploit such asymmetries, not just technological gaps, but deep institutional weaknesses [5,20]. Scholars highlight that in developing economies cyber-risk governance is often hampered by overlapping mandates, fragmented jurisdictions and weak public–private collaboration [29,30]. Moreover, financial institutions in these contexts typically struggle to align global standards like SWIFT’s customer-security controls with local reality, leading to superficial compliance and enduring exposure [15,31]. The institutional environment, shaped by underdeveloped legal regimes and a scarcity of cybersecurity professionals, further amplifies vulnerability [16,28]. The ripple effects of the heist on Bangladesh’s banking sector, such as increased cyber-risk disclosure and reactive security measures, underscore how incident experience can reshape internal practices in emerging markets [2].

Moreover, while these issues are not unique to Bangladesh, they reflect a broader pattern across the Global South, where digital-finance expansion, technological dependency and geopolitical asymmetries converge to generate cross-border cyber risk [15,28]. Addressing these challenges requires context-sensitive strategies, not mere transplantation of Global North frameworks, but a pivot toward adaptive capacity, institutional strengthening and regional cyber-governance collaboration [16,29]. Recognizing these dynamics, scholars and policymakers emphasize the need for enhanced international coordination, harmonised reporting, joint incident-response frameworks and intelligence-sharing protocols [32]. Financial institutions are urged to adopt frameworks like SWIFT’s Customer Security Programme, while governments must invest in legal and institutional capacities to combat cyber-enabled financial crime [16,31]. Whilst significant work has focused on technical vulnerabilities, malware and governance, there remain gaps in understanding how developing-country contexts bring unique permutations of risk [15]. Few studies integrate human and non-human actors in global cybercriminal ecosystems, and fewer still offer comparative or post-incident reform analyses [5,16]. To address these gaps, this study leverages the Bangladesh Bank case to deliver both theoretical insight and policy-relevant knowledge. By embedding the incident within broader cybersecurity, governance and policy debates, this study fills an urgent scholarly void and presents concrete pathways for building more resilient, adaptive and inclusive global financial systems in the era of sophisticated cyber threats. In this way, the study apparently makes three contributions.

First, it extends the cybersecurity and financial governance literature with one of the few empirically grounded analyses in a Global South context [15,31]. Second, it integrates human and non-human actors into its analytical lens, advancing socio-technical understanding of cyber-enabled financial crime. Third, it provides actionable insights for securing global financial systems, focusing on endpoint security, institutional governance and cross-border regulatory cooperation [5]. By situating the analysis within a developing country context, the study in general responded to calls for IS research to more directly address the socio-technical security challenges and institutional asymmetries faced in the Global South [33].

2. Methodology

This study employed an exploratory case study design with the 2016 Bangladesh Bank cyber heist as the focal event. Case study methodology is widely used in information systems (IS) research to investigate complex socio-technical phenomena where the boundaries between the case and its context are blurred [34,35]. Exploratory case studies are particularly appropriate when existing theory is underdeveloped, and the objective is to surface new concepts and identify gaps for further empirical research [36]. The research combined a scoping review with a critical case analysis approach. This dual method was chosen to provide both a broad theoretical understanding and an in-depth empirical examination of a specific cyber incident. The multi-layered analytical framework adopted in this study covers macro-, meso-, and micro-domains to capture the complex interplay between geopolitical, institutional, and organizational factors that contribute to cross-border cybercrime.

2.1. Scoping Review Approach

Overall, the approach represents a mix of legal analyses, technical assessments, governance frameworks, and behavioral studies. To build a theoretical foundation, a scoping review was conducted to map and synthesize the diverse body of knowledge relating to cross-border cyber risks, financial cybercrime, institutional vulnerabilities, and cybersecurity governance, particularly within developing-country contexts. Scoping reviews are particularly appropriate for emerging and multidisciplinary research domains where the objective is to identify key concepts, map existing knowledge, examine the breadth of available evidence, and identify research gaps rather than provide an exhaustive assessment of all available studies [37–39]. The theoretical framework was aimed at identifying cross-border cybersecurity risk dimensions—especially in the context of developing countries. The work of Misaki et al. [40] demonstrated the value of adapting structured review techniques to IS research in developing country contexts, reinforcing the importance of capturing both academic and grey literature. This approach provided a robust foundation for analyzing cybercrime ecosystems through a Global South lens. The overall review design was informed by the literature review guidance of Webster and Watson [41], Okoli [42], and vom Brocke et al. [43]. Consistent with these approaches, the analysis was organized around concepts and themes rather than individual authors, allowing for the development of a thematic understanding of phenomena rather than produce descriptive summaries. The outcome of this process was not only a synthesis of the state of knowledge on cybercriminal ecosystems but also the development of a set of analytical categories—termed cybersecurity risk dimensions that were subsequently applied to interpret the Bangladesh Bank heist. Thus, the scoping review was not a parallel exercise but the primary mechanism through which the conceptual framework of the study was developed and applied to the case analysis.

2.2. Search Strategy, Inclusion and Exclusion Criteria

The literature search covered both academic and grey sources to reflect the multi-dimensional nature of cybercrime risk within its ecosystems. Searches were conducted between August and September 2025 using Primo (<https://www.oru.se/university-library/find-and-borrow-material/find-material/primo-discovery-search-engine/>), a federated academic search platform subscribed to by the university where the author is also affiliated. Primo provides access to multiple scholarly databases and collections through a single search interface, including Scopus, Web of Science, HeinOnline, ScienceDirect, EconLit, EBSCOhost, JSTOR, ProQuest, Springer, Taylor & Francis, and Wiley resources, as well as books, conference proceedings, and other scholarly materials. To broaden the scope, Google Scholar was also used to retrieve additional peer-reviewed papers, investigative reports and region-specific studies. Boolean keyword combinations such as “Cyberattack in Bank”, “cybercriminal ecosystem”, “cross-border cybercrime”, “transnational cybercrime”, “financial cyberattack”, “financial cyberattack in developing countries”, “SWIFT vulnerabilities”, “cybersecurity risks in developing countries”, “characteristics of financial cybersecurity”, “cybersecurity in emerging markets”, “cyber risk governance”, and “Global South cybersecurity” guided the retrieval process that could ensure that the scoping review captures comparative Global North/South and socio-technical perspectives. Backward and forward citation tracing was used to ensure comprehensiveness [41]. The search process initially yielded 622 records. Studies were included if they: (1) addressed cybersecurity risks in the financial sector; (2) examined governance, institutional, regulatory, organizational, or socio-technical dimensions of cybersecurity; (3) provided empirical, conceptual, or policy-relevant insights applicable to developing-country contexts; or (4) were published in peer-reviewed journals, conference proceedings, or reputable institutional reports (e.g., IMF, BIS, ENISA, World Bank, SWIFT). Furthermore, exclusion criteria were applied to studies that: (1) focused exclusively on highly technical issues without organizational or governance relevance; (2) addressed cybersecurity in unrelated sectors without transferable insights for financial systems; (3) were duplicate records; or (4) lacked sufficient methodological or analytical substance. Figure 1 summarizes the literature identification, screening, and selection process. Following the removal of duplicate and clearly irrelevant records, 126 publications were retained for full-text assessment. Application of the inclusion and exclusion criteria resulted in 47 studies being included in the final synthesis. These comprised peer-reviewed journal articles, conference papers, policy documents, and investigative reports. Consistent with scoping review methodology, the search process combined predefined search terms with iterative refinement. Initial searches were guided by concepts derived from the study objectives and prior literature, while subsequent searches incorporated additional keywords and related concepts identified during the screening and review process. The identified records were then screened for relevance and assessed against the inclusion and exclusion criteria. This approach enabled a broad mapping of the multidisciplinary literature on cross-border cyber risk, financial cybersecurity, governance, and developing-country contexts. The resulting thematic synthesis informed the development of the analytical dimensions subsequently applied to the Bangladesh Bank case study.

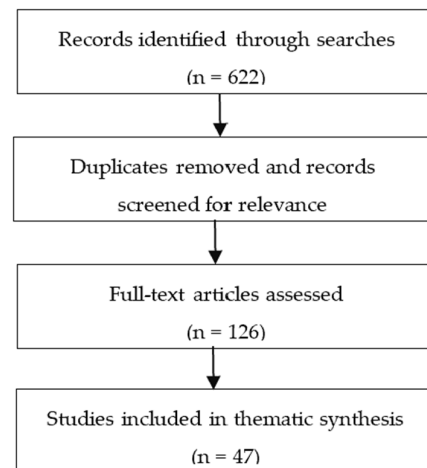


Figure 1. Study Identification and Selection Process.

2.3. Case-Specific Data Collection for the Bangladesh Bank Heist

In addition to the structured literature review, the case study of the Bangladesh Bank heist required a broader and more adaptive search strategy. Due to the limited availability of peer-reviewed scholarly work on this specific event, a supplementary Google search was conducted to identify investigative reporting, institutional publications, legal documents, and credible news coverage published from 2016 onward. These sources provided factual and contextual information regarding the sequence of events, investigative findings, and organizational responses associated with the Bangladesh Bank heist. Where available, priority was given to information reported by established institutions, official documents, and internationally recognized news organizations. Complementary academic sources were identified through databases such as EBSCOhost, and Google Scholar. However, the most detailed factual and contextual data, particularly regarding forensic evidence, vendor vulnerabilities, and post-incident responses, came from investigative journalism, whitepapers, and reports by organizations such as SWIFT, and international media. This mixed-source approach ensured a triangulated understanding of the incident, combining scholarly analysis with real-time documentation and critical commentary.

3. Literature Review—Towards a Conceptual Framework

The synthesis of the reviewed literature revealed recurring patterns of risks, vulnerabilities, and institutional responses that could be meaningfully clustered into distinct yet interdependent categories. To capture this complexity, the findings were organized into ten themes that operate across three analytical levels as shown in Table 1: macro/external environment, meso/ecosystem interactions, and micro/organizational practices. This multi-level structuring reflects how cross-border cyber risks are simultaneously shaped by geopolitical dynamics, sector-wide interdependencies, and institution-specific governance or technical practices. At the macro-level, the themes address systemic drivers such as geopolitics, national governance, regulatory regimes, financial interdependence, and critical infrastructures—factors that frame the overall threat landscape and constrain national responses. The meso-level highlights vulnerabilities that arise in the financial ecosystem, where third-party dependencies and the need for information-sharing and incident coordination influence collective resilience. Finally, the micro-level focuses on how individual financial institutions interpret, prioritize, and manage cyber risks through governance, security architecture, and human-factor management.

Table 1. Representation of the Themes.

Analytical Level	Themes
Macro/External Environment	1. Geopolitical safe-havens jurisdictions
	2. Public-sector governance
	3. Legal–regulatory gaps
	4. Cross-border financial interdependence
	5. Critical national infrastructure fragility
Meso/Ecosystem Interactions	6. Third-party vendor risk
	7. Incident coordination and threat-sharing
Micro/Organizational Practices	8. Governance and organizational risk culture
	9. Security architecture and technical control
	10. Human factors and social engineering exposure

3.1. Geopolitical Safe-Havens Jurisdictions

The *Geopolitical safe-havens* refer to the ways interstate rivalries, power asymmetries, and permissive jurisdictions create structural enablers for financial cybercrime. Safe-havens are states or territories where cybercriminal activities may occur with a lower likelihood of prosecution due to explicit protection or limited legal enforcement. Empirical evidence demonstrates that state-linked actors have repeatedly exploited geopolitical tensions to combine espionage with financially motivated attacks. The Lazarus Group campaign against SWIFT endpoints is a striking example of state-sponsored cyberattacks, where North Korean actors exfiltrated millions of dollars while reinforcing their government’s strategic objectives [44,45]. The convergence of permissive jurisdictions, i.e., the nations or regions where cybercriminals operate with minimal risk of prosecution due to lax enforcement, inadequate global enforcement mechanisms, or implicit state tolerance, and competing geopolitical interests significantly amplifies vulnerabilities in the international banking system. In this case, ‘jurisdictional arbitrage’ is a dynamic where attackers deliberately exploit regulatory gaps and jurisdictional asymmetries, shifting operations to more permissive or poorly coordinated states [46]. By taking advantage of such gaps and operating from safe-haven jurisdictions, cyber-criminals conduct sophisticated campaigns with relative impunity [47]. ENISA’s Threat Landscape stress that state-nexus groups exploit both financial infrastructures and jurisdictional fragmentation to advance hybrid objectives of espionage, sabotage, and revenue generation [48]. A study by SWIFT highlights how attackers increasingly use geopolitical cover and regulatory arbitrage to target banks in emerging markets, exploiting their dependence on international payment rails [49]. For developing economies, the consequences are especially severe as institutions are targeted via infrastructures abroad, yet governments lack both the geopolitical leverage and institutional capacity to pursue reciprocal enforcement. Together, these studies reveal that geopolitics and safe-haven jurisdictions are not peripheral issues but foundational drivers of systemic exposure to cross-border financial cybercrime.

3.2. Public-Sector Governance

The *Public-sector governance* refers to a government’s capacity to align inter-agency efforts, synchronize national priorities, and integrate financial regulation with cybersecuri-ty and development agendas. This alignment is essential to mitigating systemic exposure to cross-border financial cybercrime. Fragmented governance marked by siloed ministries, overlapping mandates, or inconsistent enforcement creates exploitable vulnerabilities. In contrast, cohesive frameworks that link financial oversight, national cybersecuri-ty strategies, and public–private coordination foster resilience and improve response

capabilities [50,51]. In developing economies in general, however, achieving such coherence remains a challenge. Weak institutional coordination or framework and inconsistent cybercrime reporting continue to undermine regional resilience, with cybercrime now constituting a substantial share of all reported offenses in many developing countries [52,53]. Institutional reforms, particularly those driven by international programs, can foster better digital and sustainable governance. Fahey [54] analyzes the evolution and divergence of EU and US cyber policies, highlighting how conflicting legislative paths impede coherent cross-border alignment. Meanwhile, Hassid [55] explores how great-power competition and institutional asymmetries act as obstacles to forming a unified global cybersecurity regime. In practice, misaligned mandates and weak coordination across states reduce deterrence, particularly in financial sectors reliant on multi-jurisdiction enforcement. Even when cross-border investigative capacity exists, fragmented legal infrastructures and mismatched rules complicate response and accountability [56]. Research indicates that limited inter-ministerial and inter-jurisdictional coordination, inconsistent adoption of national legal frameworks or cybercrime conventions, and insufficient cross-border enforcement can reduce the effectiveness of cybercrime deterrence [57,58]. Ultimately, governance coherence acts as both a shield and a structural constraint. Where institutional alignment and cross-sector integration are lacking, systemic risk persists. But when financial regulation, cybersecurity frameworks, and enforcement structures operate in tandem, the national capacity to deter and respond to cyber-enabled financial crime is significantly strengthened.

3.3. Legal–Regulatory Gaps

The *legal–regulatory gaps* refer to the robustness of national and international frameworks governing cybersecurity, anti-money laundering (AML), and cross-border enforcement mechanisms such as mutual legal assistance treaties (MLATs). This theme highlights how financial cybercrime thrives not only through technological gaps but also through legal and jurisdictional weaknesses. Outdated laws, inconsistent application, and fragmented regulatory landscapes enable cybercriminals to leverage regulatory arbitrage, obfuscate transactions, and delay prosecution across jurisdictions. Clough [59] stresses that in such fragmented conditions, mutual legal assistance becomes cumbersome, while evidentiary requirements across borders remain misaligned. Moreover, the broadening of AML mandates in advanced economies, from traditional money laundering to encompass terrorist financing, sanctions evasion, and kleptocracy, has intensified compliance pressures on financial and legal intermediaries. These gaps are even more pronounced in developing countries, where legal underdevelopment and enforcement asymmetries structurally enable financial cybercrime. Ndubueze [60] identifies that many African states have yet to fully legislate or operationalize cybercrime frameworks, resulting in patchy due diligence, weak Know Your Customer (KYC) enforcement, and opacity in beneficial ownership structures. The consequences of this legal vacuum are evident in the growing sophistication of cybercriminal networks operating within and across the region. Despite policy interest in strengthening AML and cybercrime controls, developing economies in general remain hampered by institutional capacity deficits, inconsistent enforcement, and limited cross-border cooperation. These challenges are not merely technical but structural where legal fragmentation, poor inter-agency coordination, and delayed international response mechanisms systematically reduce deterrence and embolden cybercriminal operations. In this light, regulatory and legal coherence must be understood not as a bureaucratic ideal but as a foundational requirement for defending the integrity of global financial systems in an increasingly digitized and contested geopolitical landscape.

3.4. Cross-Border Financial Interdependence

Cross-border financial interdependence is shaped by the dense networks of correspondent banking, payment infrastructures, and global settlements that bind financial systems across jurisdictions. This interconnectivity, while essential for global liquidity, creates systemic vulnerabilities since a local breach or fraudulent transaction can cascade rapidly through settlement chains, amplifying shocks across multiple markets. Beyond the technical vulnerabilities of infrastructures, recent scholarship underscores the importance of governance, regulation, and language in shaping systemic exposure. Sousa-Silva [61] states a novel forensic-linguistic dimension, demonstrating how translation technologies and manipulated communications facilitate cross-border fraud, enabling attackers to bypass linguistic and cultural barriers in financial messaging. Together, this body of work illustrates that cyber-financial interdependence is not only a matter of technical infrastructure but also of institutional asymmetries and communicative vulnerabilities.

Beyond local organizational weaknesses, cyber risk in developing-country contexts is increasingly shaped by broader structural conditions, including digital sovereignty, infrastructural dependency, and unequal participation in global technology governance. Recent scholarship argues that digital sovereignty extends beyond territorial control to encompass digital capacity, technological autonomy, and the ability to shape the infrastructures, standards, and governance arrangements upon which modern economies depend [62,63]. Developing economies frequently rely on externally developed digital infrastructures, platforms, and cybersecurity standards while possessing comparatively limited influence over their design and evolution, creating new forms of technological dependency and governance asymmetry [28]. As a result, cyber risks are shaped not only by domestic institutional weaknesses but also by asymmetric technological dependencies and uneven capacities across jurisdictions. Such conditions may constrain the ability of developing countries to effectively govern cyber risks, enforce regulatory standards, and coordinate responses to cross-border cyber incidents. Critically, without harmonized regulatory standards, stronger multilateral enforcement, and the integration of forensic tools that capture both technical and linguistic manipulation, cross-border interdependence will continue to function less as a stabilizer of global finance than as a vector of systemic fragility.

3.5. Critical National Infrastructure Fragility

Critical national infrastructure (CNI) fragility encompasses the foundational systems of telecommunications, energy grids, and internet exchange points (IXPs) that sustain the operations of modern finance. These infrastructures function as the ‘backbone layer’ for banks, payment platforms, and regulatory technologies, such that a disruption in non-financial sectors almost immediately translates into systemic financial risks. Dependence on uninterrupted electricity, stable routing through IXPs, and resilient telecommunications links positions CNI as an inseparable component of financial cyber-resilience. Ficco, Choraś, and Kozik [64] show through simulation studies that critical infrastructure failures can amplify vulnerabilities across interconnected domains. Real-world crises such as the Ukrainian power grid attack illustrate how disruption in energy systems can indirectly paralyze financial transactions, including access to SWIFT terminals and settlement platforms. Comparative evidence highlights an uneven landscape. Advanced economies often integrate redundancy and conduct cross-sector exercises within regulatory frameworks, while low- and middle-income countries remain constrained by fragile infrastructures and chronic power instability. Studies on institutional analysis [65–67] in this regard stress the need for coordinated oversight of telecom and energy infrastructures under financial cybersecurity mandates, joint simulation exercises to prepare for cascading failures, and targeted investments in redundant IXPs and backup power systems. Vedral [68] further warns

that the financial system's dependence on external infrastructures exposes it to systemic cyberattacks that transcend sectoral boundaries. Collectively, this scholarship underscores that CNI fragility is not peripheral but constitutive of financial cyber-resilience; and its weaknesses disproportionately endanger developing economies that lack redundancy, oversight, and bargaining power in global financial networks.

3.6. Third-Party Vendor Risk

The *third-party vendor risk* in financial cybersecurity refers to the systemic vulnerabilities that arise when financial institutions outsource services such as IT infrastructure, cloud computing, or payment processing to external providers. These partnerships, while offering cost efficiencies and technological agility, extend the institutional perimeter and introduce significant cybersecurity dependencies. This structural exposure becomes especially dangerous in an era of advanced persistent threats and complex global supply chains. Financial institutions increasingly rely on external vendors for critical operations, often without adequate visibility into these partners' security protocols. As Anderson-Princen [69] shows, financial institutions engaging cloud outsourcing often struggle to align internal governance with vendor controls, leaving critical operations exposed. Under the EU's DORA (Digital Operational Resilience Act), covered financial entities must revise their vendor and ICT service contracts to align with new regulatory obligations such as rights of audit, incident reporting, and subcontracting oversight thereby exposing long-standing weaknesses in vendor governance structures [70]. The challenge is even more acute in jurisdictions with weaker regulatory mandates, where banks, particularly smaller or developing-market institutions, lack the leverage or legal mandate to impose stringent cybersecurity requirements on global service providers. In developing economies, third-party risks are compounded by institutional and infrastructural deficits. As Baldoni [71] notes, low-capacity states frequently rely on imported technologies and foreign service vendors, often without adequate vetting, monitoring, or contingency planning. This creates systemic contagion risks, as a breach in one outsourced environment can cascade across interconnected financial systems. The World Bank [67] also warns that fragmented vendor oversight frameworks leave institutions vulnerable to regulatory arbitrage and cross-border attacks, especially where enforcement regimes vary significantly between countries. Scholarly consensus now points to some major imperatives for reducing these risks, such as, embedding third-party risk governance into core regulatory licensing processes in the financial sector, creating sector-wide surveillance platforms for monitoring third-party exposures, and building national or regional digital infrastructure to reduce reliance on opaque foreign providers [65,69]. Ultimately, vendor ecosystems are not tangential but central to financial cybersecurity, especially in low-resource economies where limited redundancy and oversight amplify systemic exposure.

3.7. Incident Coordination & Threat Sharing

Incident coordination and threat-sharing refer to the inter-organizational frameworks that enable financial institutions, regulators, law enforcement, and technical teams to collectively detect, analyze, and respond to cyber threats. Ultimately, coordinated information-sharing is the backbone of cyber resilience in the financial ecosystem [72,73]. In many developing countries, its underdevelopment remains a critical vulnerability that facilitates the scaling of cross-border financial cyberattacks. These mechanisms range from sector-wide security operations centers (SOCs) to bilateral information-sharing agreements and cross-border memoranda of understanding. The existence of real-time intelligence-sharing platforms reduces dwell time, constrains attacker mobility across networks, and strengthens collective incident response [74,75]. However, legal liability, data privacy concerns, and reputational

risks often deter proactive sharing, especially in jurisdictions with weak regulatory safeguards or limited trust between private and public actors. In many developing economies, the absence of institutionalized coordination platforms leaves banks reliant on foreign intermediaries or donor-driven security schemes that fail to integrate national priorities. Overall, the literature emphasizes three imperatives for ecosystem-wide resilience: (i) mandatory participation in information-sharing hubs to reduce systemic blind spots, (ii) harmonized legal standards for incident disclosure and coordination, and (iii) investment in domestic SOC to reduce dependency on foreign infrastructure and accelerate threat response. Without these, detection and response remain fragmented, especially in the context of sophisticated, cross-border cyberattacks [71,76].

3.8. Governance and Organizational Risk Culture

The *Governance and organizational risk culture* theme defines how institutions transform external and technical risks into strategic actions by allocating resources and embedding accountability. Organizational governance, leadership, and risk culture refer to the internal structures, norms, and behavioral practices through which financial institutions frame, prioritize, and manage cybersecurity risks. Governance encompasses formal oversight arrangements, including risk committees, audit functions, and board-level responsibilities, while risk culture reflects the informal behavioral dynamics that shape how cyber threats are perceived and addressed. The literature underscores that institutions with weak governance or immature risk cultures often treat cybersecurity as a siloed IT function rather than a systemic financial-stability concern resulting in reactive and fragmented responses. In contrast, institutions with strong board-level engagement and integrated cyber oversight demonstrate improved preparedness, clearer disclosure practices, and greater alignment with supervisory expectations [77]. Institutional culture and leadership behaviors further determine how governance structures translate into real-world resilience. As evident in Ghanaian context, banks with dedicated cybersecurity committees, cross-functional risk dialogues, and regular simulation exercises show superior performance in incident response [78]. Also, findings from Kenya and other emerging economies indicate that organizational readiness and cyber governance maturity are closely associated with improved productivity and adaptive capacity in the face of targeted attacks [79]. Therefore, the overarching insight is that governance and risk culture are not ancillary but foundational to effective cyber risk management. For institutions in developing countries, where infrastructural fragility and external threat exposure are elevated, embedding cybersecurity into enterprise governance and fostering a culture of transparency and accountability is vital to closing the maturity gap that enables cross-border cyberattacks.

3.9. Security Architecture and Technical Control

Security architecture and technical control refer to the degree of technical and organizational sophistication maturity within a financial institution's cybersecurity framework. This includes layered defence mechanisms, identity and access management (IAM), network segmentation, endpoint monitoring, and the integration of resilience-by-design principles. Control maturity is typically benchmarked through standards such as ISO/IEC 27001, NIST CSF, and the SWIFT Customer Security Programme (CSP), which assess whether an institution's controls are ad hoc, repeatable, defined, managed, or optimized. Studies confirm that immature or fragmented security architectures significantly elevate institutional risk, as attackers exploit outdated systems, unmonitored interfaces, and inconsistent control implementation [80,81]. Furthermore, an unsegmented infrastructure and weak endpoint monitoring facilitated unauthorized SWIFT transactions, underscoring the consequences of low control maturity [82]. Comparative analyses show that financial institutions in

advanced economies have adopted red-teaming, continuous monitoring, and regulatory stress testing to harden digital systems. In contrast, banks in low- and middle-income countries (LMICs) often struggle with budget constraints, outdated infrastructure, and limited regulatory enforcement [80]. This global disparity creates systemic risk within interconnected banking networks, where attackers can pivot through less mature jurisdictions to reach better-defended nodes. Banks with high control maturity, characterized by redundancy, regular testing, and updated playbooks, can recover within hours.

3.10. Human Factors and Social Engineering Exposure

The *Human factors and social engineering exposure* refer to vulnerabilities stemming from human behavior, cognitive biases, and organizational practices rather than technical flaws alone. In financial cybercrime, attackers frequently exploit trust relationships, weak awareness, and cultural hierarchies through phishing, pretexting, insider collusion, and credential harvesting. The central insight of this theme is that individuals—whether employees, contractors, or customers—constitute the most persistent entry vector for large-scale attacks. Pant et al. [83] analyze real-world cases of social engineering, identifying manipulation tactics that bypass even hardened security architectures by targeting cognitive and behavioral weaknesses. The persistence of social engineering threats highlights that this exposure is not just about individual lapses but stems from systemic shortcomings in awareness, culture, and governance. Overreliance on firewalls and monitoring tools without cultivating cybersecurity-conscious environments leads to a false sense of security. As recent research shows, organizational cultures that foster trust-based, non-punitive reporting environments encourage staff to flag suspicious emails or incidents early, whereas blame-oriented or punitive approaches suppress reporting and thereby heighten the risk of successful deception-based attacks [84,85]. A consensus across the literature [85–88] emphasizes that resilience against human-centric attacks depends on regular and context-specific phishing simulations, mandatory maker-checker workflows, and cross-functional engagement in fostering risk-aware cultures.

3.11. Cross-Theme Synthesis and Summary

Table 2 provides an overview of the cross-theme synthesis resulting from the literature review as stated. Cross-border financial cyber risk is not solely the result of isolated technical failures; rather, it emerges from the interplay of geopolitical factors, disparate regulatory frameworks, vulnerable critical infrastructures, and complex socio-technical dynamics within organizations. These micro-level vulnerabilities intersect with macro- and meso-level dynamics, demonstrating that cybercriminals capitalize not only on technological flaws but also on structural and organizational asymmetries. Read together, the ten themes form a layered system in which macro-level forces (geopolitics, public-sector governance, regulatory regimes, financial interdependence, and CNI) shape the threat surface and the rules of engagement; meso-level ecosystem arrangements (third-party/vendor dependencies and information-sharing/incident coordination) determine how quickly threats propagate or are contained; and micro-level institutional practices (governance and risk culture, security-control maturity, and human-factor exposure) ultimately decide whether compromises are prevented, detected, or allowed to escalate. From a developing-country perspective, these findings converge on a critical insight: large-scale financial cyberattacks succeed not merely because of isolated institutional weaknesses but due to the interaction of permissive geopolitical environments, fragmented governance systems, organizational immaturity in risk culture, i.e., uneven legal and supervisory capacity, and thin CNI redundancy (power, IXPs, backbone links). Financial institutions often depend on a narrow set of foreign correspondents and offshore vendors, while domestic information-sharing

platforms and crisis-coordination mechanisms are emergent or donor-driven. In short, resilience grows when strategy integrates the macro-rules of the game, the meso-mechanics of interdependence, and the micro-realities of organizational behavior.

Table 2. Overview of the cross-theme synthesis.

Level	Core Risk Drivers	Interdependence Dynamic	Developing Country
MACRO (External)	- Geopolitical safe-havens - Weak policy & inter-ministerial coordination - Fragmented legal regimes - Fragile CNI (power, IXPs, telecom)	- Global rails & correspondent banking spread local breaches - Coherent rules (shared-common and collective risk management) - Fragmentation (contagion conduit. Quick spread of a breach in a weak link)	- Low leverage vs. global actors - Thin CNI redundancy - Need integrated cyber-AML-finance policy
MESO (Ecosystem)	- Third-party/vendor risk - Gaps in information-sharing & incident coordination	- Shared vendors/utilities act as risk multipliers - Ecosystem rules (auditable contracts, joint drills) shape stability	- Weak vendor oversight - Donor-driven Security Operations Center (SOCs) or Computer Emergency Response Team (CERTs) - Need local hubs & harmonized disclosure
MICRO (Organizational)	- Weak board-level governance - Low technical control maturity (IAM, segmentation, monitoring, recovery) - Human-factor exposure (phishing, insider, poor reporting culture)	- Tech tools depend on behavior & governance - Gaps in: capability, coordination, and culture (cognition)	- Fast fintech/digital-finance growth outpaces maturity - Resource & skill deficits - Need enterprise-wide cyber-governance & risk-aware culture

4. Case: Bangladesh Bank Heist in 2016

4.1. Bangladesh Bank Background—Current and Pre-Heist

Bangladesh, a South Asian country on the cusp of graduating from its Least Developed Country (LDC) status in the near future, stands at a pivotal moment in its development journey. The country's banking sector plays a crucial role in supporting this growth, providing credit to the private sector, facilitating remittance inflows, and enabling trade finance. As the country's central bank, 'Bangladesh Bank' has been a cornerstone of financial governance since its establishment in 1972. As of 2026, Bangladesh has a network of over sixty-three scheduled banks, including seven state-owned commercial banks, forty-three private banks, nine foreign commercial banks, and three specialized financial institutions [89]. There is also a privately owned digital commercial bank that is currently in the process of commencing commercial operations. In addition, the five non-scheduled banks (e.g., Grameen Bank) are also under the supervision of Bangladesh Bank. As the authority responsible for monetary policy, financial oversight, and reserve management, its role is indispensable. Yet, institutional capacity issues, including limited cyber preparedness, regulatory capture, and coordination failures, have impaired its ability to proactively safeguard financial stability. Following the post-pandemic global inflation surge, rising energy import costs, and broader balance-of-payments pressures, Bangladesh's foreign

exchange reserves declined substantially from a peak of over USD 48 billion in August 2021. However, more recently, reserves have recovered gradually, supported by strong remittance inflows, positive export performance, and external financial assistance, reaching approx. USD 36 billion in gross terms and USD 31 billion under BPM6 by June 2026 [90]. This drop strained import financing capacity and highlighted broader vulnerabilities in external sector management.

In addition to its central banking and supervisory functions, Bangladesh Bank hosts the Bangladesh Financial Intelligence Unit (BFIU), which serves as the country's principal agency for anti-money laundering (AML), counter-terrorism financing (CTF), and financial intelligence activities. The BFIU is responsible for receiving and analyzing suspicious transaction reports, coordinating with domestic and international law-enforcement agencies, and supporting investigations relating to financial crimes and illicit financial flows. While the Bangladesh Bank heist was primarily a cybersecurity incident, the subsequent movement and laundering of stolen funds across multiple jurisdictions highlighted the importance of effective financial intelligence and international cooperation mechanisms in responding to cyber-enabled financial crime [91].

At the time of the 2016 heist, Bangladesh's cybersecurity and operational resilience framework for the financial sector was still evolving. Although the government had introduced a National Cybersecurity Strategy in 2014, implementation across critical financial infrastructure remained uneven, and sector-wide cyber resilience capabilities were relatively limited. Bangladesh Bank operated under ICT security and information management requirements applicable to banks and financial institutions, but these controls were primarily oriented toward information security compliance rather than comprehensive cyber resilience, threat intelligence, continuous monitoring, and coordinated incident response. Contemporary assessments indicate that Bangladesh Bank maintained poorly designed and maintained network and cybersecurity systems. Kabir [5] in this regard states "The Bangladesh Bank had four computers and four servers connected to SWIFT. Those computers and servers were also connected to the real-time gross settlement system allowing the nation's domestic banks and the central bank to perform large transfers. They were unmonitored, and the network lacked a firewall. The systems were connected to the open Internet." (p. 1). Such conditions reflected weaknesses in operational resilience, privileged-access controls, and cybersecurity governance, increasing exposure to sophisticated cross-border cyber threats. Furthermore, a dedicated Cyber Security Unit (CSU) within Bangladesh Bank was only established after the incident, highlighting the relatively immature state of institutional cybersecurity governance prior to the heist [5,20].

4.2. Overview of Bangladesh Bank Heist in 2016

Between 4 and 5 February 2016 (a Thursday–Friday weekend in Bangladesh), the offices of Bangladesh Bank in Dhaka were closed in accordance with the country's official weekend schedule. Unknown to the staff, malware that had been planted weeks earlier lay ready for strike. Cybersecurity analysts linked the heist to the highly sophisticated cyber-criminal syndicate known as the 'Lazarus Group'. The same group has also been blamed for the 2014 Sony Pictures hack, based on shared code signatures and attack methods [5,92]. The group had spent those weeks studying the bank's internal systems and SWIFT payment workflows. As shown in the timeline Figure 2 [93], late on Thursday night, as the country entered its weekend and Manila prepared for the Lunar New Year holiday, the attackers launched their operation. They sent 36 fraudulent SWIFT payment orders, attempting to steal about US \$951 million from Bangladesh Bank's account at the Federal Reserve Bank of New York [20,94]. The timing was deliberate. The Bangladeshi weekend and the holiday period in the Philippines delayed detection of suspicious transfers. Yet the attack did not

succeed completely. A spelling mistake in one beneficiary's name triggered suspicion at an intermediary Pan Asia Bank in Sri Lanka, prompting the U.S. Federal Reserve to halt most of the transfers. In the end, only five transfers, worth about US \$101 million, were executed. Within the first 48 h of the attack, approximately US \$20 million was successfully frozen and recovered from the Sri Lankan bank. In contrast, about US \$81 million was funneled through four or five transfers involving four fictitious accounts, each opened with just US \$500 nine months prior to the heist, at the Jupiter Street branch of Rizal Commercial Banking Corporation (RCBC) in the Philippines. These funds, labeled as 'consultancy fees', were quickly laundered during February and March through local casinos, exploiting regulatory loopholes in the country's anti-money laundering laws [20,94–96]. Subsequent investigations revealed the attackers' meticulous preparation. The Dridex and Carbanak malware enabled them to steal SWIFT credentials, manipulate the SWIFT Alliance Access client, erase transaction logs, and even block printer reports that would normally have alerted staff to the fraudulent activity [5,20].

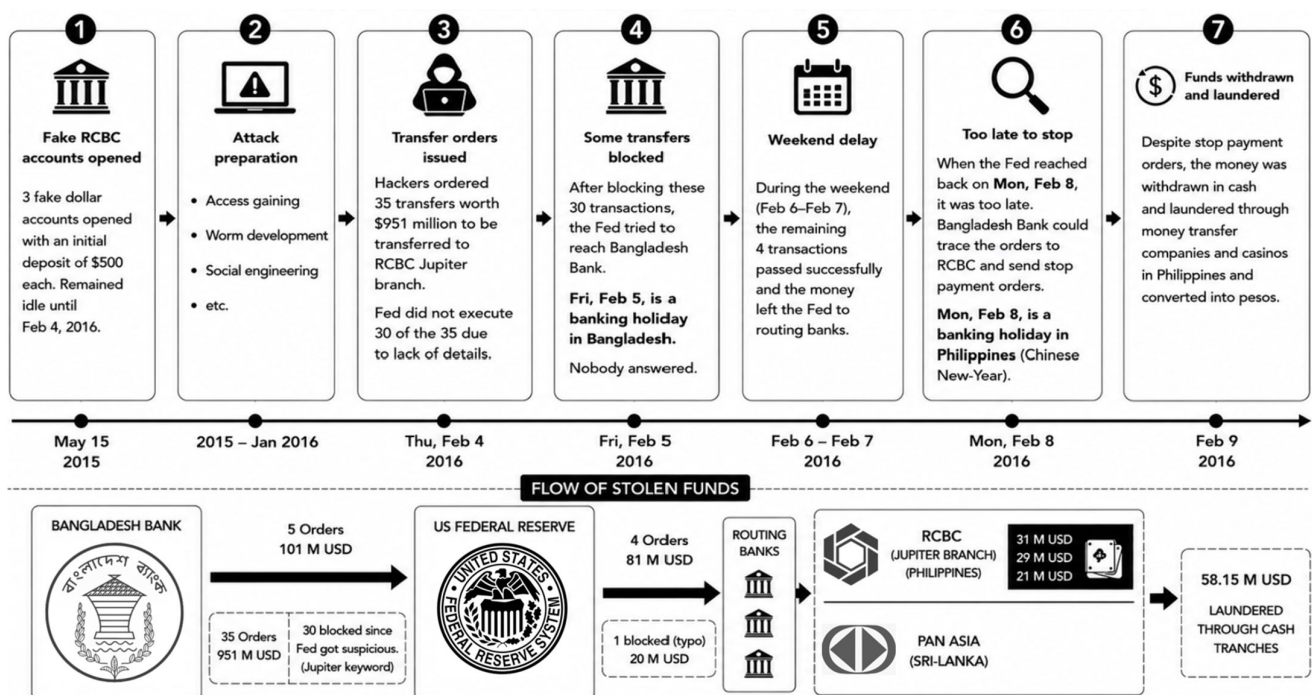


Figure 2. Graphical overview and timeline of the Attack (Image adapted from Kehrli [93]).

Public fallout was immediate and intense. The governor of Bangladesh Bank resigned amid accusations of negligence after the incident became public about a month later—not through the local media but through the *Philippine Daily Inquirer* on 15 March [97]. The senior officials were sharply criticized for their handling of the breach, as they kept the incident concealed for 24 days and took 39 days to file a case under the Money Laundering Prevention Act with the local police station [98]. Moreover, since the incident occurred in 2016, the country's Criminal Investigation Department (CID) has struggled for many years to produce a complete forensic report (95th attempt as of 18 June 2026). This prolonged delay highlights persistent institutional and technical limitations in the country's cybercrime investigation and digital forensics capacity.

Commercial banks across Bangladesh reacted by increasing disclosures of cybersecurity risks, which is an observable 'spillover effect' aimed at restoring public confidence [2]. Yet the deeper wounds were institutional: the incident exposed weak governance, poor regulatory oversight, entrenched political influence, and the lack of strong leadership to manage both the internal crisis and the complex international repercussions.

4.2.1. Geopolitics & Safe-Haven Jurisdictions

The Bangladesh Bank heist highlights how geopolitical asymmetries and permissive financial jurisdictions shape the risk landscape for cross-border cyber-enabled theft. Evidence links the operation to the Lazarus Group, reflecting how a sanctioned state actor weaponized cyber-crime for revenue [95,99]. Attackers exploited regulatory loopholes in safe-haven jurisdictions, notably the Philippines, where, at the time, casinos were exempt from AML reporting, allowing the swift layering of the stolen US \$81 million [5,100,101]. The absence of robust cross-border legal assistance treaties, fragmented AML supervision, and uneven SWIFT-security compliance impeded rapid tracing and recovery [102,103]. Bangladesh's limited political and economic leverage constrained its ability to compel cooperation from stronger counterparts such as the U.S. Federal Reserve or Philippine authorities [2]. The case shows that cyber-crime thrives at the intersection of geopolitics, offshore finance, and regulatory arbitrage, demanding closer global AML alignment, coordinated cyber-forensics, and sanction-aware financial supervision.

4.2.2. Public-Sector Governance

The Bangladesh Bank heist exposed deep structural weaknesses in public-sector governance and policy coherence that magnified the crisis and delayed recovery efforts. At the time of the incident, Bangladesh lacked a standing inter-agency cyber-incident response mechanism, forcing ministries, law-enforcement agencies, and the central bank to act in institutional silos, often working at cross-purposes [104]. This fragmentation hampered swift coordination with the New York Federal Reserve, SWIFT authorities, and Philippine regulators during the critical early hours of the attack. Pervasive political patronage in senior appointments and entrenched corruption further eroded the Bangladesh Bank's institutional autonomy, weakened its regulatory authority, and undermined its credibility in both domestic and international financial circles [100]. Reports from investigative journalists and inquiries alleged that some senior officials and influential local figures exerted pressure on the central bank's leadership, delaying disclosure of the heist and shielding certain officials from accountability, thereby compounding the crisis and eroding public trust [105–107]. Instead of a unified, transparent crisis-management framework, the government resorted to ad hoc blame-shifting, internal reshuffles, and delayed parliamentary oversight, undermining the central bank's ability to lead the response [98,100]. The CID's prolonged forensic investigation, which failed to deliver a conclusive report for several years, highlighted the enduring institutional bottlenecks in investigating and prosecuting sophisticated cyber-financial crimes [108]. The Bangladesh case demonstrates that policy coherence, strong central-bank independence, and effective inter-agency coordination, backed by credible political stewardship, are essential for crisis readiness in an era of state-linked, cross-border cybercrime. Absent these capacities, even a technically sophisticated financial system can become highly vulnerable to coordinated cyber-enabled theft.

4.2.3. Regulatory & Legal Gaps

At the time of the Bangladesh Bank heist, the country's regulatory and legal regime was marked by fragmentation, institutional inertia, and an alarming absence of modern cybersecurity governance standards. Bangladesh Bank and regulator lacked both the statutory mandate and operational infrastructure to enforce cybersecurity across the financial sector. The MLA treaties and cross-border cooperation protocols were weak, slowing coordination with the U.S. Federal Reserve, Philippine regulators, and international investigators [95,103]. Moreover, the Bangladesh Financial Intelligence Unit (BFIU) had limited institutional autonomy and enforcement capacity, further weakening the AML ecosystem. Jurisdictional mismatches and lengthy diplomatic procedures impeded timely freezing

of stolen funds. The laundering pathway was facilitated by the absence of coordinated oversight between central banks, law enforcement, and casino regulators, both domestically and abroad [100,102]. The lack of legal provisions for cyber forensic investigation and absence of inter-agency protocols contributed to this opacity. Reports later confirmed that the bank did not have an internal cybersecurity unit or dedicated chief information security officer (CISO) at the time of the attack—further reflecting a systemic neglect of cyber risk [102]. The heist revealed deep structural failings in Bangladesh’s financial governance and regulatory architecture. The regulatory regime lacked mandatory cyber-incident reporting requirements, baseline security standards for banks, and dedicated legal mechanisms for prosecuting state-linked cyber-attacks. These deficiencies left systemic vulnerabilities latent until the crisis exposed them, illustrating how inadequate legal and institutional preparedness can magnify the consequences of cross-border financial cyber-crime.

4.2.4. Cross-Border Financial Interdependence

The heist highlighted how interconnected global payment infrastructures can be turned into vectors of systemic risk. By breaching a peripheral but weakly protected node, Bangladesh Bank, the Lazarus Group weaponized the trusted SWIFT network, using it to send 36 fraudulent orders to the Federal Reserve Bank of New York [95,109]. Bangladesh’s structural reliance on correspondent banking for U.S. dollar settlement meant that, once the fraudulent instructions left Dhaka, it had little operational leverage to halt or recall the transfers [100,101]. Such a dependency turned the global rails of trust into a vector of vulnerability. Notably, the fraudulent instructions were initially rejected due to formatting errors but later corrected and resubmitted; yet the system, lacking robust automated cross-checks, still processed them. The reversal of one transaction (typo in “Shalika Foundation” as “Fandation”) occurred only because Deutsche Bank, acting as an intermediary, flagged the irregularity that underscored how human compliance in the chain acted as the final firewall amid weak automated safeguards [96,110,111]. This interdependency, unaccompanied by enforceable norms or shared accountability, turned global financial connectivity from a strength into a liability. As highlighted by Huang and Madnick [1], without synchronized legal frameworks or harmonized technical standards, mandatory incident-reporting, and credible cross-jurisdictional cooperation attackers will continue to exploit jurisdictional blind spots and systemic weak links within the cross-border financial architecture. Developing countries like Bangladesh, structurally reliant on Western financial intermediaries for dollar clearing, often operate within an asymmetrical system where authority is centralized, but accountability for cyber-resilience is not.

4.2.5. Critical National Infrastructure (CNI) Fragility

Although the heist did not directly target telecom or power grids, its success relied on the integrity of the ICT backbone, stable connectivity, and reliable routing operations [112]. The broader South Asian region, including Bangladesh, faces persistent challenges in hardening its critical infrastructure against cyber threats, with limited redundancy and aging digital assets reducing systemic resilience [113–115]. The heist case exposed how weaknesses in a country’s ICT backbone can indirectly enable high-impact financial crimes. The country’s lower infrastructure resilience reduced the chance of detecting suspicious transfers in real time and hampered incident response. The limited redundancy in backbone networks and dependence on a few international links increased the attack surface. During the heist, delayed alerts and poor log visibility reflected infrastructural fragility that constrained the central bank and law-enforcement agencies. Investigations revealed that the central bank operated without a firewall and used secondhand \$10 switches or routers in its SWIFT room, severely undermining the perimeter defenses [116,117]. Such cheap and

unsegmented network hardware made it difficult for forensic investigators to trace intrusion paths and allowed attackers to move laterally with little resistance. In effect, the bank's reliance on minimal, low-cost networking gear exposed the SWIFT interface, and thus its global payment capabilities, to exploitation. Bangladesh's broader infrastructure ecosystem magnified these technical weaknesses. The limited visibility of internal that demonstrated infrastructural fragility constrained Bangladesh Bank's ability to mount an effective defense or forensic response. Because the network core was not hardened or monitored at multiple layers, attackers could manipulate software, such as the SWIFT client, while suppressing print logs and audit trails [106]. The absence of a robust national Critical Infrastructure Protection regime and the limited reach of BGD e-Gov CIRT further hindered cross-sector coordination. Unlike jurisdictions with resilient and redundant ICT systems, Bangladesh's infrastructural gaps amplified the attackers' operational window, underscoring the need for systemic investments in backbone resilience, real-time monitoring, and coordinated institutional response [118,119] (The Financial Express, 2024; BGD e-Gov CIRT, n.d.).

4.2.6. Third-Party Vendor Risk

The 2016 heist starkly demonstrated how third-party software vulnerabilities and lax vendor governance can become critical points of failure in financial cybersecurity [120]. Forensic investigations revealed that attackers exploited security flaws in the locally deployed SWIFT Alliance Access system by embedding malware that allowed them to intercept, modify, and delete transaction records and print logs [20,106]. The malware, linked to the Lazarus Group, infiltrated the bank's network through a vendor-supplied software update, bypassing internal validation due to the absence of multi-layered audit controls or code-signing mechanisms [95,121]. Investigative reports uncovered systemic vendor management gaps, including the absence of rigorous due diligence, poor enforcement of software patch policies, and limited segregation of access rights [111,122–124]. There were indications that certain foreign consultants were granted elevated system access without formal security vetting or contractual constraints, potentially compromising sensitive operational zones [5,121,125]. These consultants reportedly operated within a compromised procurement environment characterized by limited oversight and political influence, raising concerns about insider risks and regulatory blind spots [124]. Critically, the attackers connected to the SWIFT system, tampered with SWIFT transaction logs by disabling printers, ensuring that no physical record of the fraudulent transactions would alert staff the following morning [106]. In this way the attackers leveraged such a weak vendor ecosystem to conceal fraudulent transfers. This manipulation of both software and hardware components highlights how attackers exploited fragmented vendor governance and inadequate endpoint security. The incident underscores a key lesson for financial institutions in low-capacity jurisdictions: without enforceable vendor contracts, secure integration protocols, continuous monitoring, and supply chain transparency, third-party arrangements can shift from operational enablers to systemic liabilities.

4.2.7. Incident Coordination and Threat-Sharing

The Bangladesh Bank heist laid bare the severe gaps in cyber incident coordination and cross-border information-sharing that persist in many developing economies [126]. At the time of the attack, Bangladesh Bank operated largely in isolation from the broader global cyber-threat intelligence ecosystem. Despite the existence of global platforms like the SWIFT secure operations center and sector-specific Computer Emergency Response Teams (CERTs), there seem to be no automated channels or active protocols for real-time information exchange between the bank and its international counterparts [127]. During the critical hours of the heist, efforts to verify or stop the fraudulent SWIFT transfers were

delayed not only by the time zone differences and holiday calendars in Bangladesh and the Philippines, but also by the absence of structured escalation paths with key institutions such as the Federal Reserve Bank of New York [128]. The heist exposed a critical lack of structured communication and institutional coordination, with responses relying heavily on informal emails, delayed verifications, and the absence of pre-negotiated crisis protocols or MOUs, which are the factors that significantly delayed detection and response efforts [5]. This fragmented response enabled attackers to move money through casinos and third-party accounts before regulatory action could be coordinated. Further compounding the issue, investigations revealed that intelligence and technical updates were often shared late or withheld due to bureaucratic silos, inter-agency rivalry, and lack of trust both domestically and across borders [121]. Such coordination failures highlight the need for institutionalized frameworks for cyber crisis response that include multi-stakeholder drills, secure communication channels, and trust-based intelligence-sharing agreements, especially in developing financial systems that are becoming increasingly digitized and globally integrated.

4.2.8. Governance and Organizational Risk Culture

The heist revealed severe weaknesses in the governance structure and cybersecurity risk culture of the central bank. Cybersecurity was not treated as a strategic priority, and crisis-response mechanisms were underdeveloped. An institutional culture shaped by political patronage and corruption encouraged risk-avoidance and bureaucratic caution rather than proactive incident-handling, undermining both detection and response [2,100]. Staff were left without clear escalation protocols or institutional readiness to detect and contain sophisticated breaches [103]. The absence of timely communication and coordination among senior officials further exacerbated the problem. Then-Governor reportedly concealed news of the heist for 24 days from the Government's concerned Offices, which is an omission harshly criticized by the then government appointed investigation committee as a breach of protocol and institutional accountability [129]. The committee was formed on March 15, about two weeks after the 'Philippine Daily Inquirer' first reported the cyber theft. According to internal accounts, the delay stemmed from fears of reputational damage and uncertainty over fund recovery strategies, but it also reflected broader cultural deficiencies in transparency and risk governance of the bank.

The leadership vacuum was particularly pronounced in the domain of cybersecurity oversight. At the time of the breach, the central bank lacked a centralized cybersecurity function or a designated Chief Information Security Officer (CISO), resulting in missed alerts and poor inter-departmental coordination. Red flags, such as the printer malfunction in the SWIFT room, were dismissed without escalation. It was, however, not until four years later (May 2020) that Bangladesh Bank established a dedicated Cyber Security Unit (CSU) to formalize security leadership and develop institutional capabilities. This long-delayed structural response highlights how institutional inertia, politicized leadership, and the absence of accountability mechanisms can significantly delay organizational learning and expose national financial systems to prolonged risk [98,100].

4.2.9. Security Architecture and Technical Control

The heist exposed that, technically, the bank's control environment was far below the maturity expected of a systemically important financial institution. The SWIFT gateway was directly connected to the broader internal network, lacking proper network segmentation, layered defences, or zero-trust safeguards [102,109]. Critical monitoring tools, such as anomaly detection, logging, and alerting, were either poorly configured or deliberately disabled by the malware, allowing attackers to erase printer logs and suppress SWIFT

transaction alerts [20,100]. There is no indication that the Bank had implemented red teaming exercises, threat-hunting activities, or regular resilience testing prior to the incident, reflecting a low level of cybersecurity control maturity at the time [95,103]. Due to a reactive and poorly coordinated control environment, the attackers were able to stay inside the system for several weeks before carrying out the theft, successfully avoiding detection and counter response. The absence of independent anomaly detection, end-to-end audit trails, and resilience stress testing left the system vulnerable to persistent, state-level operators. Such findings confirm that for high-stakes financial nodes, true cyber-resilience demands architecture built for segmentation, secure logging, independent monitoring, and continuous stress testing [130].

4.2.10. Human Factors and Social Engineering Exposure

The Bangladesh Bank heist illustrates how human factors can become the weakest link in cybersecurity. Initial access likely came through social engineering or credential compromise. Internal staff awareness, training, and procedural discipline were weak. The attackers further undermined the human oversight layer by manipulating system outputs so that even checking staff could be misled. Investigations later revealed that as early as January 2015, several bank employees received deceptive emails from an individual calling himself 'Rasel Ahlam', who claimed to be seeking a job and invited recipients to click on a link to download a CV and cover letter. According to BBC News [96], this link is suspected to have contained malware that enabled remote access, offering attackers an entry point into the bank's internal systems. This is an early sign of alarmingly low levels of staff cyber-awareness and a lack of effective phishing-resistance programs. This lapse underscored the vulnerability of the human layer, as no robust mechanism existed to educate staff, or encourage prompt reporting of suspicious emails. Despite handling critical financial infrastructure, the bank lacked a mature cybersecurity training or awareness program or clear internal protocols for responding to phishing attempts. Once inside the network, the attackers were able to escalate their intrusion and exploit technical weaknesses, such as by manipulating the SWIFT Alliance Access system, suppressing print logs, and falsifying transaction messages, thereby deceiving even the employees tasked with oversight [20,130]. A work culture was apparently characterized by hesitation and fear of reprisal. The absence of a culture that encourages reporting questionable behaviors compounded the failure. In this way, the human and process layers became collateral damage in the attacker's strategic design. The case, therefore, demonstrates a cautionary tale that a robust cybersecurity requires not only firewalls and software patches, but also empowered personnel, shared responsibility, and a culture that incentivizes vigilance and procedural transparency.

5. Discussion and Conclusions

The Bangladesh Bank heist stands as one of the most revealing cases of how cross-border cyber risks, when compounded by weak governance and institutional fragility, can culminate in a coordinated and large-scale financial cyberattack. This heist was not an entirely isolated incident within the national context. Subsequent reports and assessments identified additional cyber incidents affecting financial institutions and public-sector organizations in Bangladesh, although none matched the scale or international significance of the 2016 reserve theft. While much attention has focused on the technical breach itself, the deeper story is one of institutional breakdown. The incident reflects long-standing structural vulnerabilities within Bangladesh's banking and governance systems marked by corruption, regulatory capture, and politically motivated appointments. These conditions created an environment where accountability mechanisms were weakened, leadership was reactive and risk-averse, and strategic oversight was virtually absent. Rather than

responding with decisive coordination, government and institutional actors defaulted to internal blame-shifting, resignations, and rhetorical damage control. Investigative efforts, such as the CID's delayed and limited forensic reporting, were hampered by bureaucratic inertia and a lack of prosecutorial follow-through [131]. The process of recovering stolen funds has been slow and incomplete, and many of the original digital footprints remain untraced. This failure to mobilize an effective response underscores that the heist was not merely a cyber intrusion but a symptom of a broader governance failure -where weak rule of law, institutional opacity, and leadership paralysis left no buffer for crisis resilience. The event also exposed the layered nature of cybercriminal ecosystems, which thrive not only on technological failure but on the fragmentation of geopolitical norms, inconsistencies in legal-regulatory regimes, fragile national infrastructures, and limited cross-agency coordination. These risks intersect and reinforce one another, creating systemic exposures that adversaries can exploit with precision. What emerges from the Bangladesh case is a multi-dimensional picture of cyber risk that cannot be explained by technology alone. The following synthesis builds on these insights by organizing the findings into three levels of analysis: macro (geopolitical and regulatory), meso (institutional and ecosystem), and micro (organizational and human factors) as also outlined in Table 3. This layered approach not only explains how the attack succeeded but also highlights several theoretical and practical gaps in current frameworks for understanding and mitigating cybercrime in low-governance contexts.

Table 3. Synthesis of the Bangladesh Bank case and lessons learned.

Themes	Key Insights from Bangladesh Case	Theoretical Relevance in Other Contexts	Lessons Learned & Recommendations
Geopolitical safe havens	Hackers exploited international regulatory gaps; limited prosecution capacity. Weak jurisdictions like the Philippines enabled laundering and shielded attackers.	Jurisdictional arbitrage; enforcement asymmetry	Strengthen regional MLATs and participate in cyber diplomacy/prosecution capabilities to close legal loopholes.
Public-sector governance	Lack of inter-agency coordination; slow response due to bureaucratic silos; and poor cyber-policy integration.	Policy incoherence; institutional fragmentation	Establish national cyber crisis coordination centers with defined escalation paths in financial and national strategies.
Legal-regulatory gaps	Fragmented legal frameworks, ineffective AML regimes, and weak cross-border legal cooperation.	Legal asymmetries, AML enforcement deficits, transnational regulatory lag	Harmonize cybercrime and AML frameworks; strengthen MLATs and evidence protocols.
Cross-border financial interdependence	High reliance on SWIFT system and correspondent banks without systemic cyber-risk mitigation.	Asymmetric interdependence, contagion pathways, digital liquidity risk	Enhance controls over high-value transactions; integrate anomaly detection into SWIFT systems.
Critical infrastructure fragility	Lack of redundant IT systems and insecure IXPs created system-level vulnerabilities.	Infrastructure fragility, sectoral interdependence, resilience deficit	Build redundancy and cyber-incident drills into telecom, disaster recovery and power infrastructure linked to finance.

Table 3. *Cont.*

Themes	Key Insights from Bangladesh Case	Theoretical Relevance in Other Contexts	Lessons Learned & Recommendations
Third-party vendor risk	Compromised local vendor introduced malware into SWIFT environment.	Trust asymmetry; Vendor governance/ dependency gaps, risk externalization, outsourcing vulnerabilities	Mandate third-party audits, enforce security clauses in vendor contracts. AML compliance for non-traditional financial intermediaries.
Incident coordination & threat-sharing	Poor or no channel to share alerts with SWIFT; real-time intelligence sharing or international banks quickly.	Information asymmetry, institutional mistrust, cross-border blind spots	Develop financial-CERT alliances and incident playbooks.
Governance & organizational risk culture	Weak oversight, passive leadership, and fear-driven culture prevented escalation.	Governance immaturity, accountability vacuum, reactive risk culture	Foster cyber-risk governance through leadership training and simulations. Embed cyber risk governance at board-level and link KPIs to resilience indicators.
Security architecture & technical controls	Weak endpoint controls, unsegmented systems, outdated network security, and no red-teaming practices.	Control maturity gaps, outdated security protocols, cyber hygiene deficits	Adopt context-aware cyber hygiene baselines; Align control standards to NIST/SWIFT CSP and prioritize segmentation.
Human factors & social engineering exposure	Phishing and social engineering bypassed basic defenses due to low staff awareness.	Behavioral vulnerabilities; awareness shortfall, human-centric attack vector	Continuous simulation-based awareness training to improve detection and reporting; launch sector-wide anti-phishing campaigns.

At the geopolitical level, jurisdictions such as the Philippines and Sri Lanka functioned as permissive transit zones for illicit financial flows, owing to weak enforcement regimes and limited international cooperation mechanisms. The Lazarus Group exploited these fragmented legal and regulatory landscapes to evade sanctions and obscure attribution [132,133]. Despite multiple red flags, intermediaries such as RCBC in the Philippines processed suspicious transactions over several days without meaningful intervention [20,96]. Much of the theoretical literature emphasizes cyber-espionage or state-directed attacks, yet it has not fully accounted for how geopolitical safe havens actively enable transnational, financially motivated cybercrime. The issue is fundamentally geopolitical because it involves the strategic behavior of states, acting as both enablers and targets, within an uneven international order. Diverging national interests, uneven capacity, and the lack of harmonized cyber norms allow certain states to become either passive enablers or at times willing participants in laundering schemes. The Bangladesh case further highlights a persistent enforcement asymmetry: the country lacked both the bilateral legal tools and the geopolitical leverage needed to compel timely international cooperation.

Policy coherence and institutional readiness were also critically lacking in Bangladesh's response. The absence of a coordinated inter-agency mechanism delayed incident escalation, hindered communication with the U.S. Federal Reserve, and created confusion about the respective roles of the Ministry of Finance, the central bank, and law enforcement [92].

In contrast to models in developed countries, where national cybersecurity centers and real-time response playbooks are in place, developing states such as Bangladesh still operate in fragmented silos. The literature often assumes the existence of institutional capacity for integrated cyber-governance; this case demonstrates how such assumptions break down in practice. Bangladesh's regulatory and legal environment has also been notably fragile. Historically, weak AML enforcement and the absence of active MLATs created a ready pathway for laundering by attackers [59,134]. The country's original cybercrime framework, rooted in the ICT Act of 2006 and modestly amended in 2013, suffered from vague provisions, weak enforcement, and misalignment with global norms. The Digital Security Act of 2018 continued many of these shortcomings, including broad powers, ambiguous definitions, and limited safeguards [135–137]. The then regime faced widespread criticism for failing to provide the clarity, enforceability, or cross-border cooperation mechanisms needed to prosecute complex financial cybercrime [138]. Following the fall of the long-standing regime in 2024, which had ruled for 15 years since 2009, the interim government formally repealed the Cyber Security Act of 2023 and introduced a new Cyber Security Ordinance in October 2025. Although this shift signals an intention to reform and modernize the country's cyber-legal framework, doubts remain about whether the new ordinance can adequately address entrenched problems of weak enforcement, legal ambiguity, and limited international coordination that continue to undermine Bangladesh's capacity to confront sophisticated cross-border cyber threats [139]. A comparable example can be seen in the Philippines, which long excluded casinos from its AML jurisdiction, thereby creating a legal loophole exploited by criminal actors. Such cases underscore the limitations of prevailing theories on global regulatory compliance, which often overlook how financial crimes thrive in legal grey zones and in the absence of synchronized enforcement across jurisdictions.

At the institutional, or meso-level, over-reliance on the SWIFT system and global payment infrastructures demonstrated how digital interdependence, while efficient, becomes a vulnerability when not accompanied by sufficient cybersecurity and governance capacity [31]. Attackers used fraudulent instructions to access Bangladesh's reserves held at the U.S. Federal Reserve. The role of interbank payment chains and "weak connectors," such as linguistic errors and routing anomalies [106], has been under-explored in the literature, particularly in developing-world contexts. Third-party vendor risk emerged as a critical attack vector, with malware reportedly introduced into Bangladesh Bank's SWIFT environment through a compromised vendor software update [20,140]). The bank lacked robust audit processes, had no visibility into vendor code, and possessed no enforceable security clauses in its contracts. Vendor-governance frameworks for low-capacity countries remain under-theorized, even as outsourcing increases in these contexts. Information-sharing was also alarmingly slow. Bangladesh lacked a formal channel to coordinate cyber-incidents with SWIFT, U.S. law enforcement, or regional CERTs [5,134]. The literature frequently assumes the presence of trust, institutional maturity, and legal safe harbors for intelligence-sharing, assumptions that do not hold in fragile states, where agencies may fear political fallout or reputational damage.

At the micro-organizational level, Bangladesh Bank's internal weaknesses magnified the damage. There was a lack of cybersecurity-governance structure at the board level, no central risk oversight, and poor incident-escalation capacity. Technical controls such as network segmentation, anomaly detection, and access restrictions were either absent or disabled [140,141]. In such environments, best-practice standards such as NIST or ISO remain largely aspirational due to funding and skill constraints. Human error also played a decisive role. Social-engineering tactics, notably phishing, were used to gain access, and once inside, attackers manipulated logs to evade detection. Internal staff hesitated to raise alarms due to a culture of fear and punitive response [84,86,94]. Despite the growing field of

behavioral cybersecurity, there remains limited understanding of how institutional culture, accountability gaps, and weak digital literacy shape risk behavior in the Global South.

5.1. Post-Heist Reforms and Institutional Responses

The Bangladesh Bank heist in February 2016 triggered a series of institutional, regulatory, and organizational reforms that extended well beyond the affected institution. Consistent with broader research on cyber resilience and financial-sector governance [16,27], the incident exposed the limitations of relying solely on technical safeguards and highlighted the need for stronger governance, oversight, and institutional coordination. In response, Bangladesh Bank strengthened cybersecurity oversight and supervisory practices, while SWIFT introduced its Customer Security Programme (CSP) in May 2016 and Customer Security Controls Framework (CSCF) to establish a common security baseline, enhance threat-intelligence sharing, and improve fraud detection across the global financial network [141]). In fact, this heist is widely cited as a landmark case that exposed weaknesses in the cybersecurity governance of globally interconnected financial infrastructures and subsequently informed international efforts to strengthen operational resilience, information sharing, and security standards across the SWIFT ecosystem [5,141]. These developments reflected a growing recognition that cyber resilience depends not only on technology but also on effective governance structures, organizational preparedness, and coordinated risk-management practices. The long-term consequences of this heist further underscore the institutional dimensions of cyber risk. Ongoing forensic investigations, legal proceedings, and international recovery efforts demonstrate the complexity of responding to transnational cybercrime. As of May 2026, the submission of the investigation report had been deferred for the 95th time, highlighting the prolonged legal and investigative challenges associated with the case. According to a news report [142], the CID finalized the charge sheet, naming 64 individuals and organizations from Bangladesh and abroad. The accused include the then Governor and ten other bank officials of Bangladesh Bank, and individuals and entities from the Philippines, Sri Lanka, China, Japan, India, and North Korea (incl. hacker Park Jin-hyuk—a core member and operative of the ‘Lazarus Group’). An expatriate cybersecurity expert who served as an IT consultant to Bangladesh Bank under the Financial Sector Support Project and was later appointed as the lead forensic auditor to investigate the security breach was also charged with allegedly tampering with or destroying forensic evidence. All those charges are based on forensic evidence, FBI reports, SWIFT data, international cooperation records, recovered-fund documentation, and witness statements. On the other hand, progress has been made in recovering some stolen assets. According to the CID and court records, approximately USD 20 million was recovered from Sri Lanka, around USD 68,000 was returned through the Rizal Commercial Banking Corporation (RCBC) in the Philippines, and an additional USD 14 million was recovered through various initiatives. More recently, a Dhaka court ordered the confiscation and recovery of approximately USD 81 million held at RCBC [142]. More broadly, the Cyber Security Ordinance 2025 introduced updated provisions relating to critical information infrastructure protection, cybercrime enforcement, incident reporting, digital evidence management, and inter-agency cooperation. In February 2025, Bangladesh Bank also introduced the ‘Cybersecurity Framework 1.0’, which was developed based on the six core functions of the NIST Cybersecurity Framework, such as, Govern, Identify, Protect, Detect, Respond, and Recover. The framework is aligned with the National ICT Security Policy, the ICT Security Guidelines of Bangladesh Bank, and relevant international standards [143]. Taken together, these developments suggest a gradual shift from reactive cybersecurity practices toward a more integrated model of cyber-risk governance and financial-sector

resilience, while illustrating how major cyber incidents can catalyze institutional learning, regulatory adaptation, and organizational transformation [5].

5.2. Applicability to Other Developing-Country Contexts

While the Bangladesh Bank heist provides the empirical foundation for this study, the identified risk dimensions appear relevant beyond the Bangladeshi context. Similar patterns have been observed in other cyber-enabled financial crimes across developing and emerging economies. For example, the 2018 Cosmos Bank cyberattack (estimated loss approx. USD 13.5 million) in India exposed weaknesses in payment infrastructure, governance controls, third-party dependencies, and incident-response mechanisms, ultimately facilitating coordinated fraudulent withdrawals across multiple jurisdictions [126]. Likewise, the attempted cyber theft from Vietnam's Tien Phong Bank in 2015 (USD 1.1 million) demonstrated how vulnerabilities in SWIFT-connected systems could be exploited to initiate fraudulent cross-border transfers, although timely intervention prevented substantial losses [1,49]. Comparable weaknesses were also evident in the Banco del Austro case in Ecuador in 2015 (USD 12 million), where attackers leveraged compromised credentials and deficiencies in cross-border payment oversight to execute unauthorized international transfers [1]. More recently, incidents involving NIC Asia Bank in Nepal in 2017 (USD 4.4 million) and a growing number of cyber-enabled financial crimes across South and Southeast Asia have highlighted how limited cyber governance capacity, fragmented regulatory oversight, uneven cybersecurity maturity, and weak cross-border coordination continue to create opportunities for transnational cybercriminal networks [8,52]. Similar themes can also be observed in attacks targeting financial institutions in Chile, where operational disruptions exposed the interconnected nature of cyber resilience, governance, and incident coordination within globally integrated financial systems [48]. Although these incidents differ in scale, institutional context, and technical execution, they collectively suggest that cyber-enabled financial crime cannot be understood solely through technological vulnerabilities. Rather, recurring weaknesses relating to governance capacity, institutional coordination, regulatory effectiveness, critical infrastructure resilience, third-party dependencies, and organizational cyber maturity appear across multiple contexts [1,16,27,126]. These common patterns reinforce the argument that institutional fragility remains a critical determinant of cyber risk in developing-country financial systems. Consequently, the multi-level framework proposed in this study should be viewed not as a Bangladesh-specific explanation, but as a transferable analytical lens for examining how geopolitical conditions, regulatory structures, ecosystem interdependencies, and organizational practices interact to shape cross-border cyber risk across diverse developing-country contexts.

5.3. Concluding Remarks

This study makes a theoretical contribution by integrating the domains of cybersecurity, international development, and governance into a single explanatory model. While existing literature often examines technical or regulatory aspects in isolation, this research highlights the interplay of geopolitical positioning, institutional incoherence, and organizational immaturity in facilitating cross-border cybercrime. It offers a comprehensive risk framework that is analytically layered yet adaptable to other country contexts. Importantly, the study addresses a long-standing gap in the literature: despite the scale and symbolism of the Bangladesh Bank heist in 2016, no academic study had undertaken a full-spectrum critical analysis of its enabling conditions and systemic implications until now. For policymakers and practitioners, the findings suggest that cyber-resilience must extend beyond technical defences to include coordinated legal frameworks, robust vendor oversight, and institutionalized incident-response protocols. Bangladesh's experience

demonstrates that ad hoc approaches to cyber-incidents, dependent on informal networks and delayed diplomacy, are inadequate in an era where cybercrime operates transnationally, at speed, and often with state complicity. The study further emphasizes the need to harmonize national cybersecurity strategies with financial oversight, especially in developing economies undergoing rapid digital transformation.

Nevertheless, the research has limitations. It relies largely on secondary data due to the restricted availability of official forensic and legal documentation. Although the analysis draws on triangulated sources, including academic literature, investigative journalism, and institutional reports, some dimensions of the attack remain obscured by political sensitivities and opaque disclosures. Furthermore, the Bangladesh context may not fully generalize to higher-capacity developing countries or to regions with distinct regulatory and technological landscapes. The presented analytical framework, while theoretically grounded, would benefit from empirical validation across multiple jurisdictions. Future work could therefore extend these insights through comparative studies of developing countries facing similar cyber-risk exposures. Primary data collection, particularly interviews with financial institutions, law-enforcement agencies, and cybersecurity experts, would further enhance understanding of institutional readiness and response dynamics. In addition, deeper examination of the roles played by international regulatory bodies such as SWIFT, FATF, and the IMF in shaping cybersecurity-compliance and enforcement norms could reveal new levers for cross-border governance reform. With digital financial inclusion advancing rapidly across the Global South, scholars must also investigate how these developments intersect with emerging cyber-threat vectors, particularly in contexts marked by institutional fragility and weak oversight.

As a conclusive reflection, the Bangladesh Bank heist is not merely a cautionary tale of one nation's vulnerability but a global signal, an alarm echoing from Dhaka to Manila, revealing the cracks in the firewall of an interconnected yet uneven digital-financial landscape. Unless countries align cybersecurity with governance and legal strategy, they will remain exposed not only to attacks but to cascading systemic risks.

Funding: The Open access publication funding was supported by the Office of Research & Innovation at Alfaisal University.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The author declares no conflicts of interest.

References

1. Huang, K.; Madnick, S.M. *Cyber Securing Cross-Border Financial Services*; Working Paper No. SMAD-2020-17; MIT Sloan School of Management: Cambridge, MA, USA, 2020. Available online: <https://web.mit.edu/smadnick/www/wp/2020-17.pdf> (accessed on 17 October 2025).
2. Mazumder, M.M.M.; Sobhan, A. The spillover effect of the Bangladesh Bank cyber heist on banks' cyber risk disclosures in Bangladesh. *J. Oper. Risk* **2021**, *15*, 53–76. [CrossRef]
3. Perdana, A.; Aminanto, E. Hack, heist, and havoc: The Lazarus Group's triple threat to global cybersecurity. *J. Inf. Technol. Teach. Cases* **2024**, *16*, 206–217. [CrossRef]
4. Adelman, F.; Elliott, J.A.; Ergen, I.; Gaidosch, T.; Jenkinson, N.; Khiaonarong, T.; Morozova, A.; Schwarz, N.; Wilson, C. *Cyber Risk and Financial Stability: It's a Small World After All*; IMF Staff Discussion Note No. 2020/007; International Monetary Fund: Washington, DC, USA, 2020. [CrossRef]

5. Kabir, M.S.A. Lessons learned from the Bangladesh Bank heist. *ISACA J.* **2023**, *6*, 1–4. Available online: <https://www.isaca.org/resources/isaca-journal/issues/2023/volume-6/lessons-learned-from-the-bangladesh-bank-heist> (accessed on 6 December 2023).
6. Uddin, M.H.; Ali, M.H.; Hassan, M.K. Cybersecurity hazards and financial system vulnerability: A synthesis of literature. *Risk Manag.* **2020**, *22*, 239–309. [CrossRef]
7. Bruce, M.; Lusthaus, J.; Kashyap, R.; Phair, N.; Varese, F. Mapping the global geography of cybercrime with the World Cybercrime Index. *PLoS ONE* **2024**, *19*, e0297312. [CrossRef] [PubMed]
8. United Nations Office on Drugs and Crime (UNODC). *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape*; UNODC Regional Office for Southeast Asia and the Pacific (ROSEAP): Bangkok, Thailand, 2024. Available online: https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf (accessed on 17 October 2025).
9. Mushtaq, S.; Shah, M. Threats to the Digital Ecosystem: Can Information Security Management Frameworks, Guided by Criminological Literature, Effectively Prevent Cybercrime and Protect Public Data? *Computers* **2025**, *14*, 219. [CrossRef]
10. Caltagirone, S.; Pendergast, A.; Betz, C. *The Diamond Model of Intrusion Analysis*; Technical Report; Center for Cyber Intelligence Analysis and Threat Research: Langley, VA, USA, 2013. Available online: <https://apps.dtic.mil/sti/pdfs/ADA586960.pdf> (accessed on 17 October 2025).
11. Broadhead, S. The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. *Comput. Law Secur. Rev.* **2018**, *34*, 1180–1196. [CrossRef]
12. Dupont, B. The governance of cybercrime: An ecological approach. *Can. J. Criminol. Crim. Justice* **2024**, *66*, 1–23. Available online: <https://utppublishing.com/doi/10.3138/cjccj-2024-0034> (accessed on 17 October 2025). [CrossRef]
13. Zhou, Y.; Tiwari, M.; Bernot, A.; Lin, K. Metacrime and cybercrime: Exploring the convergence and divergence in digital criminality. *Asian J. Criminol.* **2024**, *19*, 419–439. [CrossRef]
14. Cyber UK. Nation State Hackers Case Study: Bangladesh Bank Heist. Cyber.UK. Available online: <https://cyber.uk/areas-of-cyber-security/cyber-security-threat-groups-2/nation-state-hackers-case-study-bangladesh-bank-heist/> (accessed on 17 October 2025).
15. Świątkowska, J. *Tackling Cybercrime to Unleash Developing Countries' Digital Potential*; Pathways for Prosperity Commission Background Paper Series, No. 33; Oxford University: Oxford, UK, 2020. Available online: https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2020-01/tackling_cybercrime_to_unleash_developing_countries_digital_potential.pdf (accessed on 17 October 2025).
16. International Monetary Fund (IMF). *Cyber Risk: A Growing Concern for Macroeconomic Stability*. In *Global Financial Stability Report, April 2024*; International Monetary Fund (IMF): Washington, DC, USA, 2024; Chapter 3. Available online: <https://www.imf.org/-/media/Files/Publications/GFSR/2024/April/English/ch3.ashx> (accessed on 17 October 2025).
17. Acar, A.; Lu, L.; Uluagac, A.S.; Kirda, E. An analysis of malware trends in enterprise networks. In *Information Security*; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2019; Volume 11719, pp. 231–255. [CrossRef]
18. Sfetcu, N. *Advanced Persistent Threats in Cybersecurity—Cyber Warfare*; MultiMedia Publishing: Mumbai, India, 2024. [CrossRef]
19. Muller, L.P. *Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities*; Norwegian Institute of International Affairs: Oslo, Norway, 2014.
20. Balu, R. *Bangladesh Bank Heist: Incident Analysis*; Georgia Institute of Technology Repository: Atlanta, GA, USA, 2016. Available online: <https://repository.gatech.edu/server/api/core/bitstreams/df3d1c19-47be-4738-a855-9c049b709d52/content> (accessed on 17 October 2025).
21. Kaspersky Lab. *Lazarus Under the Hood* (Cyber Vault Library Report). 2017. Available online: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180244/Lazarus_Under_The_Hood_PDF_final.pdf (accessed on 17 October 2025).
22. North, D.C. *Institutions, Institutional Change and Economic Performance*; Cambridge University Press: Cambridge, UK, 1990. [CrossRef]
23. Scott, W.R. *Institutions and Organizations: Ideas, Interests, and Identities*, 4th ed.; SAGE Publications: Thousand Oaks, CA, USA, 2014.
24. Acemoglu, D.; Robinson, J.A. *Why Nations Fail: The Origins of Power, Prosperity, and Poverty*; Random House: New York, NY, USA, 2012.
25. Fukuyama, F. Commentary. *Governance* **2013**, *26*, 347–368. [CrossRef]
26. Ewoh, P.; Vartiainen, T. Vulnerability to cyberattacks and sociotechnical solutions for health care systems: Systematic review. *J. Med. Internet Res.* **2024**, *26*, e46904. [CrossRef] [PubMed]
27. Bank for International Settlements (BIS). *Cyber-Resilience: Range of Practices*; Basel Committee on Banking Supervision, Bank for International Settlements (BIS): Basel, Switzerland, 2018. Available online: <https://www.bis.org/bcbis/publ/d454.pdf> (accessed on 17 October 2025).

28. United Nations Conference on Trade and Development (UNCTAD). *Digital Economy Report 2021: Cross-Border Data Flows and Development—For Whom the Data Flow*; UNCTAD/DER/2021; United Nations: Geneva, Switzerland, 2021. Available online: <https://unctad.org/page/digital-economy-report-2021> (accessed on 17 October 2025).
29. North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence (CCDCOE). *Cybersecurity Governance and Normative Frameworks: Non-Western Countries and International Organizations Perspectives*; CCDCOE: Tallinn, Estonia, 2024. Available online: <https://ccdcoe.org/library/publications/cybersecurity-governance-and-normative-frameworks-non-western-countries-and-international-organizations-perspectives/> (accessed on 17 October 2025).
30. Fidler, M. Fragmentation of International Cybercrime Law. *Utah Law Rev.* **2025**, *2025*, 737. [CrossRef]
31. Aldasoro, I.; Gambacorta, L.; Giudici, P.; Leach, T. *The Drivers of Cyber Risk*; BIS Working Paper No. 865; Bank for International Settlements: Basel, Switzerland, 2020. Available online: <https://www.bis.org/publ/work865.pdf> (accessed on 17 October 2025).
32. Maurer, T.; Nelson, A. *International Strategy to Better Protect the Financial System Against Cyber Threats*; Carnegie Endowment for International Peace: Washington, DC, USA, 2020.
33. Walsham, G. South–South and triangular cooperation in ICT4D. *Electron. J. Inf. Syst. Dev. Ctries.* **2020**, *86*, e12130. [CrossRef]
34. Benbasat, I.; Goldstein, D.K.; Mead, M. The Case Research Strategy in Studies of Information Systems. *MIS Q.* **1987**, *11*, 369–386. [CrossRef] [PubMed]
35. Yin, R.K. *Case Study Research and Applications: Design and Methods*, 6th ed.; SAGE Publications: Thousand Oaks, CA, USA, 2018.
36. Stebbins, R.A. *Exploratory Research in the Social Sciences*; SAGE Publications, Inc.: Thousand Oaks, CA, USA, 2001. [CrossRef]
37. Arksey, H.; O'Malley, L. Scoping studies: Towards a methodological framework. *Int. J. Soc. Res. Methodol.* **2005**, *8*, 19–32. [CrossRef]
38. Levac, D.; Colquhoun, H.; O'Brien, K.K. Scoping studies: Advancing the methodology. *Implement. Sci.* **2010**, *5*, 69. [CrossRef] [PubMed]
39. Tricco, A.C.; Lillie, E.; Zarin, W.; O'Brien, K.K.; Colquhoun, H.; Levac, D.; Moher, D.; Peters, M.D.J.; Horsley, T.; Weeks, L.; et al. PRISMA Extension for Scoping Reviews (PRISMA-ScR): Checklist and explanation. *Ann. Intern. Med.* **2018**, *169*, 467–473. [CrossRef] [PubMed]
40. Misaki, E.; Apiola, M.; Gaiani, S.; Tedre, M. Challenges facing sub-Saharan small-scale farmers in accessing farming information through mobile phones: A systematic literature review. *Electron. J. Inf. Syst. Dev. Ctries.* **2018**, *84*, e12034. [CrossRef]
41. Webster, J.; Watson, R.T. Analyzing the past to prepare for the future: Writing a literature review. *MIS Q.* **2002**, *26*, xiii–xxiii. Available online: <http://www.jstor.org/stable/4132319> (accessed on 17 October 2025). [CrossRef]
42. Okoli, C. A guide to conducting a standalone systematic literature review. *Commun. Assoc. Inf. Syst.* **2015**, *37*, 879–910. [CrossRef]
43. vom Brocke, J.; Simons, A.; Riemer, K.; Niehaves, B.; Plattfaut, R.; Cleven, A. Standing on the shoulders of giants: Challenges and recommendations of literature search in information systems research. *Commun. Assoc. Inf. Syst.* **2015**, *37*, 205–224. [CrossRef]
44. Groll, E. NSA Official Suggests North Korea Was Culprit in Bangladesh Bank Heist. *Foreign Policy*, 21 March 2017. Available online: <https://foreignpolicy.com/2017/03/21/nsa-official-suggests-north-korea-was-culprit-in-bangladesh-bank-heist/> (accessed on 17 October 2025).
45. Volkov, D. *Lazarus Arisen: Architecture, Techniques and Attribution*; Group-IB: Singapore, 2017. Available online: <https://www.group-ib.com/lazarus.html> (accessed on 17 October 2025).
46. Draganidis, S. Jurisdictional arbitrage: Combatting an inevitable by-product of cryptoasset regulation. *J. Financ. Regul. Compliance* **2023**, *31*, 170–185. [CrossRef]
47. Corbet, S.; Gurdgiev, C. Financial digital disruptors and cyber-security risks: Paired and systemic. *Forthcom. J. Terror. Cyber Insur.* **2017**, *1*, 1–20. [CrossRef]
48. ENISA. *ENISA Threat Landscape: Finance Sector, January 2023 to June 2024*; European Union Agency for Cybersecurity: Brussels, Belgium, 2024; ISBN 978-92-9204-677-4. [CrossRef]
49. Carter, W.A. *Forces Shaping the Cyber Threat Landscape for Financial Institutions*; SWIFT Institute Working Paper No. 2016-004; SSRN: Amsterdam, The Netherlands, 2017. Available online: <https://ssrn.com/abstract=3047730> (accessed on 17 October 2025).
50. Latorcai, C.J.; Strausz, P.; Csödö, Z. Impact of institutional change programs on digital and sustainable public sector governance. *Int. J. Public Sect. Manag.* **2025**, *38*, 610–626. [CrossRef]
51. Qudus, L. Cybersecurity governance: Strengthening policy frameworks to address global cybercrime and data privacy challenges. *Int. J. Sci. Res. Arch.* **2025**, *14*, 1146–1163. [CrossRef]
52. INTERPOL. *Africa Cyberthreat Assessment Report 2025*, 4th ed.; International Criminal Police Organization (INTERPOL): Lyon, France, 2025.
53. Iwasaki, I.; Kočenda, E. Corporate crime in European emerging markets. *Borsa Istanbul. Rev.* **2025**, *25*, 1270–1292. [CrossRef]
54. Fahey, E. The evolution of EU–US cybersecurity law and policy. *Eur. Integr.* **2024**, *6*, 1073–1088. [CrossRef]
55. Hassid, N.; Matania, E. A global regime for cybersecurity and the obstacles to future progress. *Glob. Gov.* **2024**, *30*, 13–40. [CrossRef]

56. Casino, F.; Samobre, V.; Tuosto, E. SoK: Cross-border criminal investigations and digital evidence. *J. Cybersecur.* **2022**, *8*, tyac014. [CrossRef]
57. Abraha, H.H. Law enforcement access to electronic evidence across borders: Mapping policy approaches and emerging reform initiatives. *Int. J. Law Inf. Technol.* **2021**, *29*, 118–153. [CrossRef]
58. Mishra, A.; Alzoubi, Y.I.; Anwar, M.J.; Gill, A.Q. Attributes impacting cybersecurity policy development: An evidence from seven nations. *Comput. Secur.* **2022**, *120*, 102820. [CrossRef]
59. Clough, J. *Principles of Cybercrime*; Cambridge University Press: Cambridge, UK, 2020. [CrossRef]
60. Ndubueze, P.N. Cybercrime and legislation in an African context. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*; Holt, T.J., Bossler, A.M., Eds.; Palgrave Macmillan: London, UK, 2020; pp. 345–361. [CrossRef]
61. Sousa-Silva, R. ‘We attempted to deliver your package’: Forensic translation in the fight against cross-border cybercrime. *Int. J. Semiot. Law* **2024**, *37*, 1323–1349. [CrossRef]
62. Musoni, M.; Karkare, P.; Teevan, C.; Domingo, E. *Global Approaches to Digital Sovereignty: Competing Definitions, Contrasting Policy Approaches*; ECDPM Discussion Paper No. 344; European Centre for Development Policy Management: Maastricht, The Netherlands, 2023.
63. Jiang, M. Models of state digital sovereignty from the Global South: Diverging experiences from China, India and South Africa. *Policy Internet* **2024**, *16*, 727–738. [CrossRef]
64. Ficco, M.; Choraś, M.; Kozik, R. Simulation platform for cyber-security and vulnerability analysis of critical infrastructures. *J. Comput. Sci.* **2017**, *22*, 179–186. [CrossRef]
65. Financial Stability Board (FSB). *Effective Practices for Cyber Incident Response and Recovery*; FSB Publications; FSB: Basel, Switzerland, 2020. Available online: <https://www.fsb.org/uploads/P191020-1.pdf> (accessed on 17 October 2025).
66. International Monetary Fund. *The Cybersecurity Challenge to Financial Stability*; IMF Publications; IMF: Washington, DC, USA, 2021.
67. World Bank. *Strengthening Cybersecurity and Resilience of Critical Infrastructure: Insights from the Republic of Korea and Other Digital Nations*; Innovation & Technology Note Series No. 10; World Bank Korea Office: Incheon, Republic of Korea, 2023. Available online: <https://documents1.worldbank.org/curated/en/099705012152346616/pdf/IDU044546588061b004aaf08b5805c55aee4128.pdf> (accessed on 17 October 2025).
68. Vedral, B. The vulnerability of the financial system to a systemic cyberattack. In *Proceedings of the 13th International Conference on Cyber Conflict (CyCon)*; NATO CCDCOE: Tallinn, Estonia, 2021. Available online: https://ccdcoe.org/uploads/2021/05/CyCon_2021_Vedral.pdf (accessed on 17 October 2025).
69. Anderson-Princen, J.M. Cloud outsourcing in the financial sector: An assessment of internal governance strategies on a cloud transaction between a bank and a leading cloud service provider. *Eur. Bus. Organ. Law Rev.* **2022**, *23*, 905–936. [CrossRef]
70. Buttigieg, C.P.; Zimmermann, B.B. The Digital Operational Resilience Act: Challenges and some reflections on the adequacy of Europe’s architecture for financial supervision. *ERA Forum* **2024**, *25*, 11–28. [CrossRef]
71. Baldoni, R. Managing the cyber risk in a multipolar world. *Int. J. Crit. Infrastruct. Prot.* **2022**, *39*, 100578. [CrossRef]
72. Azad, M.A.; Bag, S.; Ahmad, F.; Hao, F. Sharing is caring: A collaborative framework for sharing security alerts. *Comput. Commun.* **2021**, *165*, 75–84. [CrossRef]
73. Oriola, O.; Adeyemo, A.B.; Papadaki, M.; Kotzé, E. A collaborative approach for national cybersecurity incident management. *Inf. Comput. Secur.* **2021**, *29*, 457–484. [CrossRef]
74. Johnson, C.; Badger, L.; Waltermire, D.; Snyder, J.; Skorupka, C. *Guide to Cyber Threat Information Sharing*; NIST Special Publication 800-150; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2016. Available online: <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-150.pdf> (accessed on 17 October 2025).
75. Roobini, M.S.; Chowdary, M.B.; Srinivas, Y.; Jayanthi, S.; Srividhya, E. Cloud based threat intelligence sharing for collective defence. In *Proceedings of the Ninth International Conference on Science, Technology, Engineering and Mathematics (ICONSTEM 2024)*; IEEE: New York, NY, USA, 2024; pp. 1–6. [CrossRef]
76. Ali, A.; Shah, M.; Foster, M.; Alraja, M.N. Cybercrime resilience in the era of advanced technologies: Evidence from the financial sector of a developing country. *Computers* **2025**, *14*, 38. [CrossRef]
77. Cheng, S.; Li, J.; Luo, L.; Zhu, Y. Cybersecurity governance and digital finance: Evidence from sovereign states. *Financ. Res. Lett.* **2024**, *60*, 105533. [CrossRef]
78. Opuni-Frimpong, J.; Dzorka, M.A.; Boadi, I. Governance’s role in bank performance: Cybersecurity committee assessment. *J. Financ. Report. Account.* **2025**, *23*, 788–810. [CrossRef]
79. Tetteh, G.; Otioma, C. Cyberattack, cyber risk mitigation capabilities, and firm productivity in Kenya. *Small Bus. Econ.* **2025**, *64*, 1493–1514. [CrossRef]
80. Mashizha, M.; Kanengoni, P. The adequacy of cybersecurity in financial institutions in Zimbabwe. *Int. Res. J. Bus. Stud.* **2024**, *17*, 317–331. [CrossRef]
81. Pöyhönen, J.; Lehto, M. Architecture framework for cyber security management. In *Proceedings of the European Conference on Cyber Warfare and Security*; Academic Conferences International Ltd.: Reading, UK, 2024; Volume 23, p. 2340. [CrossRef]

82. Polishchuk, V.; Fedirko, N.; Grytsyshen, D.; Ohdanskyi, K.; Kotkovskyy, V. Stability of financial institutions under the influence of cyber threats. *OIDA Int. J. Sustain. Dev.* **2025**, *18*, 11–18. Available online: <https://ssrn.com/abstract=5344609> (accessed on 17 October 2025).
83. Pant, V.K.; Pant, J.; Singh, R.K.; Srivastava, S. Social engineering in the digital age: A critical examination of attack techniques, consequences, and preventative measures. In *Effective Strategies for Combatting Social Engineering in Cybersecurity*; Kumar, R., Srivastava, S., Elngar, A., Eds.; IGI Global Scientific Publishing: Hershey, PA, USA, 2025; pp. 61–76. [CrossRef]
84. Ben Naseir, M.A.; Dogan, H.; Apeh, E.; Richardson, C.; Ali, R. Contextualising the national cyber security capacity in an unstable environment: A Spring Land case study. In *New Knowledge in Information Systems and Technologies: WorldCIST '19 2019*; Rocha, Á., Adeli, H., Reis, L., Costanzo, S., Eds.; Springer: Cham, Switzerland, 2019; Volume 930, pp. 373–382. [CrossRef]
85. Sutton, A.; Tompson, L. Towards a cybersecurity culture-behaviour framework: A rapid evidence review. *Comput. Secur.* **2025**, *148*, 104110. [CrossRef]
86. Benson, V.; McAlaney, J.; Frumkin, L.A. Emerging threats for the human element and countermeasures in current cyber security landscape. In *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications*; IGI Global: Hershey, PA, USA, 2019; pp. 1264–1269.
87. Marshall, N.; Sturman, D.; Auton, J.C. Exploring the evidence for email phishing training: A scoping review. *Comput. Secur.* **2024**, *139*, 103695. [CrossRef]
88. Khadka, K.; Ullah, A.B. Human factors in cybersecurity: An interdisciplinary review and framework proposal. *Int. J. Inf. Secur.* **2025**, *24*, 119. [CrossRef]
89. Bangladesh Bank. Banks & FCs. 2026. Available online: <https://www.bb.org.bd/en/index.php/financialactivity/bankfi> (accessed on 20 June 2026).
90. Dhaka Tribune. Bangladesh's Forex Reserves Hit 43-Month High of \$35.63bn. Dhaka Tribune, 15 June 2026. Available online: <https://www.dhakatribune.com/business/412662/bangladesh%E2%80%99s-forex-reserves-hit-43-month-high-of> (accessed on 17 June 2026).
91. Bangladesh Financial Intelligence Unit (BFIU). *Bangladesh Financial Intelligence Unit Annual Report 2023–2024*; Bangladesh Bank: Dhaka, Bangladesh, 2024. Available online: https://www.bfiu.org.bd/pdf/pub/annual/bfiu_2023-24.pdf (accessed on 20 June 2026).
92. Nish, A. What Links the 2016 Bangladesh Bank Heist to the Sony Pictures Hack? *WIRED*, 27 May 2016. Available online: <https://www.wired.com/story/adrian-nish-threat-intelligence/> (accessed on 17 October 2025).
93. Kehrli, J. Deciphering the Bangladesh Bank Heist. *NiceIdeas*. 2017. Available online: <https://www.niceideas.ch/roller2/badtrash/entry/deciphering-the-bengladesh-bank-heist> (accessed on 17 October 2025).
94. Karim, Y.; Hasan, R. Taming the digital bandits: An analysis of digital bank heists and a system for detecting fake messages in electronic funds transfer. In *Advances in Intelligent Systems and Computing*; Sandhu, R.M., Ed.; Springer: Cham, Switzerland, 2020; Volume 1271, pp. 193–210. [CrossRef]
95. US Department of Justice (DOJ). Criminal Complaint. AO 91 (Rev. 11/11). 8 June 2018. Available online: <https://www.justice.gov/archives/opa/press-release/file/1092091/dL> (accessed on 17 October 2025).
96. BBC News. The Lazarus Heist: How North Korea Almost Pulled Off a Billion-Dollar Hack. *BBC*, 27 June 2021. Available online: <https://www.bbc.com/news/stories-57520169> (accessed on 17 October 2025).
97. Inquirer. PH blocks \$870M Stolen from Bangladesh. *Philippine Daily Inquirer*, 9 March 2016. Available online: <https://business.inquirer.net/208243/ph-blocks-870m-stolen-from-bangladesh> (accessed on 17 October 2025).
98. Guardian. Bangladesh Bank Governor Resigns Over \$81m Cyber Heist. *The Guardian*, 15 March 2016. Available online: <https://www.theguardian.com/world/2016/mar/15/bangladesh-central-bank-governor-resigns-over-81m-dollar-cyber-heist> (accessed on 17 October 2025).
99. Ji-Young, K.; Jong In, L.; Kyoung Gon, K. The all-purpose sword: North Korea's cyber operations and strategies. In *Proceedings of the 2019 11th International Conference on Cyber Conflict (CyCon)*; IEEE: New York, NY, USA, 2019; pp. 1–20. [CrossRef]
100. Quadir, S.; Aneez, S.; Bergin, T.; Layne, N.; Das, K.N.; Spicer, J. The Bangladesh Bank Heist. *Reuters*, 10 March 2017. Available online: <https://2017.sopawards.com/wp-content/uploads/2017/03/The-Bangladesh-Bank-Heist.pdf> (accessed on 17 October 2025).
101. The New York Times. Bangladesh's Billion-Dollar Bank Heist. *The New York Times Magazine*, 3 May 2018. Available online: <https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html> (accessed on 17 October 2025).
102. KPMG. Bangladesh Hack Illustrates Rising Sophistication of Attacks. August 2016. Available online: <https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2016/08/swift-it.pdf> (accessed on 17 October 2025).
103. Khan, A.; Malaika, M. *Central Bank Risk Management, Fintech, and Cybersecurity*; IMF Working Paper No. 2021/105; International Monetary Fund (IMF): Washington, DC, USA, 2021. [CrossRef]

104. Hossain, Z.; Zaman, G.K.; Taher, K.A. Cyber Emergency Response Team for Bangladesh. In *Proceedings of the 2021 International Conference on Information and Communication Technology for Sustainable Development (ICICT4SD)*; IEEE: New York, NY, USA, 2021; pp. 477–480. [CrossRef]
105. Barrett, D.; O’Keeffe, K. FBI Suspects Insider Involvement in \$81 Million Bangladesh Bank Heist. *The Wall Street Journal*, 10 May 2016. Available online: <https://www.wsj.com/articles/fbi-suspects-insider-involvement-in-81-million-bangladesh-bank-heist-1462861549> (accessed on 17 October 2025).
106. Quadir, S. Exclusive: Bangladesh Panel Finds Insiders Negligent in Central Bank Heist. *Reuters*, 8 December 2016. Available online: <https://www.reuters.com/article/us-cyber-heist-bangladesh-exclusive-idUSKBN13X1S4> (accessed on 17 October 2025).
107. Kalbela. Two Ministers Served as the “Protective Shield” for the Masterminds Behind the Reserve Heist. *Kalbela*, 3 January 2025. Available online: <https://www.kalbela.com/ajkerpatrika/firstpage/152564> (accessed on 17 October 2025). (In Bangla)
108. TBS Report. Reserve Heist: Submission of Probe Report Deferred for 89th Time. *The Business Standard*, 29 September 2025. Available online: <https://www.tbsnews.net/bangladesh/reserve-heist-submission-probe-report-deferred-89th-time-1248636> (accessed on 17 October 2025).
109. BAE Systems. Two Bytes to \$951M: Investigating the Bangladesh Bank Cyber-Heist. April 2016. Available online: <https://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html> (accessed on 17 October 2025).
110. CNBC. *How a Hacker’s Typo Helped Stop a Billion Dollar Bank Heist*; CNBC: Englewood Cliffs, NJ, USA, 2016. Available online: <https://www.cnbc.com/2016/03/10/how-a-hackers-typo-helped-stop-a-billion-dollar-bank-heist.html> (accessed on 17 October 2025).
111. Das, K.N.; Spicer, J. How the New York Fed Fumbled over the Bangladesh Bank Cyber-Heist. 21 July 2016. Available online: <https://www.reuters.com/investigates/special-report/cyber-heist-federal> (accessed on 17 October 2025).
112. Bouveret, A. *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment*; IMF Working Paper No. WP/18/143; International Monetary Fund: Washington, DC, USA, 2018. Available online: <https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924> (accessed on 17 October 2025).
113. Raska, M.; Ang, B. *Cybersecurity in Southeast Asia; Note de Présentation No. 5/8, Observatoire Asie du Sud-Est*; Asiacentre/Centre Asie: Paris, France, 2018. Available online: https://asiacentre.eu/wp-content/uploads/2021/11/NotePresentation-AngRaska-Cybersecurity_180518.pdf (accessed on 17 October 2025).
114. Mukherjee, M.; Abhinay, K.; Rahman, M.M.; Yangdhen, S.; Sen, S.; Adhikari, B.R.; Nianthi, R.; Sachdev, S.; Shaw, R. Extent and evaluation of critical infrastructure, the status of resilience and its future dimensions in South Asia. *Prog. Disaster Sci.* **2023**, *17*, 100275. [CrossRef]
115. UNESCAP. Critical Analysis of ICT Connectivity in Rural Bangladesh: Importance, Constraints and Way Forward. 2024. Available online: <https://www.unescap.org/kp/2024/critical-analysis-ict-connectivity-rural-bangladesh-importance-constraints-and-way-forward> (accessed on 17 October 2025).
116. Finextra. No Firewall and \$10 Routers Blamed in Bangladesh Bank Heist. 22 April 2016. Available online: <https://www.finextra.com/newsarticle/28784/no-firewall-and-10-routers-blamed-in-bangladesh-bank-heist> (accessed on 17 October 2025).
117. Reuters. Bangladesh Bank Exposed to Hackers by Cheap Switches, No Firewall [News Article]. *Reuters*, 13 May 2016. Available online: <https://www.reuters.com/article/technology/bangladesh-bank-exposed-to-hackers-by-cheap-switches-no-firewall-police-idUSKCN0XI1UN> (accessed on 17 October 2025).
118. The Financial Express. Cybersecurity in Critical Information Infrastructure of Bangladesh. 13 May 2024. Available online: <https://thefinancialexpress.com.bd/views/cybersecurity-in-critical-information-infrastructure-of-bangladesh> (accessed on 17 October 2025).
119. BGD e-Gov CIRT. Bangladesh e-Government Computer Incident Response Team. Available online: <https://www.cirt.gov.bd/> (accessed on 17 October 2025).
120. Peng, J. The intricate web of third-party cybersecurity risk. *ISACA J.* **2023**, *6*, 55–58. Available online: <https://www.isaca.org/resources/isaca-journal/issues/2023/volume-6/the-intricate-web-of-third-party-cybersecurity-risk> (accessed on 17 October 2025).
121. Buchanan, B. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*; Oxford University Press: Oxford, UK, 2017.
122. Patterson Belknap Webb & Tyler LLP. Lessons from the Bangladesh Central Bank Heist. *Lexology*, 5 April 2016. Available online: <https://www.lexology.com/library/detail.aspx?g=9e20a200-9570-48bb-97a0-e055c4007a94> (accessed on 17 October 2025).
123. Shah, N.U. Central Bank Gets Rid of Stigma. *The Asian Age (Bangladesh)*, 17 January 2023. Available online: <https://dailiasianage.com/news/300324/central-bank-gets-rid-of--stigma> (accessed on 17 October 2025).
124. Daily Sun. Bangladesh Bank Heist: Rakesh Asthana Remains a Mystery. *Daily Sun*, 18 August 2025. Available online: <https://www.daily-sun.com/post/242925> (accessed on 17 October 2025).
125. Schwartz, M.J. Bangladesh Bank Heist Probe Finds ‘Negligent’ Insiders. *BankInfoSecurity*, 9 December 2016. Available online: <https://www.bankinfosecurity.com/bangladesh-bank-heist-probe-finds-negligent-insiders-a-9586> (accessed on 17 October 2025).
126. Maurer, T.; Nelson, A. The global cyber threat to financial systems. In *Finance & Development*; IMF: Washington, DC, USA, 2021.

127. TBS Report. Most Banks Still Lack Measures Against Cyber-Attacks. *The Business Standard*, 20 October 2020. Available online: <https://www.tbsnews.net/economy/banking/most-banks-still-lack-measures-against-cyber-attacks-147592> (accessed on 17 October 2025).
128. Corkery, M. Hackers' \$81 Million Sneak Attack on World Banking. *The New York Times*, 30 April 2016. Available online: <https://www.nytimes.com/2016/05/01/business/dealbook/hackers-81-million-sneak-attack-on-world-banking.html> (accessed on 17 October 2025).
129. Prothom Alo. Atiur Rahman Kept BB Heist Secret for 24 Days. *Prothom Alo*, 29 January 2019. Available online: <https://en.prothomalo.com/bangladesh/Atiur-Rahman-kept-BB-heist-secret-for-24-days> (accessed on 17 October 2025).
130. Bangladesh Bank. Progress on the Process of Recovering the Funds Stolen from Bangladesh Bank Through Cyber Hacking and Related Activities Under Various Initiatives. Official Press Release. 22 October 2017. Available online: https://www.bb.org.bd/mediaroom/press_release/press/oct222017_reshacking.pdf (accessed on 17 October 2025). (In Bangla)
131. Chowdhury, Z. BB Heist Case: CID Fails to Produce Forensic Probe Report in 7 Years. *The Business Standard*, 26 December 2022. Available online: <https://www.tbsnews.net/bangladesh/crime/bb-heist-case-cid-fails-produce-forensic-probe-report-7-years-557450> (accessed on 17 October 2025).
132. Sanger, D.E.; Kirkpatrick, D.D.; Perlroth, N. The World Once Laughed at North Korean Cyberpower. No More. *The New York Times*, 15 October 2017. Available online: <https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html> (accessed on 17 October 2025).
133. Perlroth, N. *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race*; Bloomsbury Publishing: London, UK, 2021.
134. Yaeger, M.L.; Goldstein, M.G.R.; Monty, K. The Bangladesh cyberheist: How compliance programs can help protect against cybercrime. *Hedge Fund J.* **2016**, *114*. Available online: <https://thehedgefundjournal.com/the-bangladesh-cyberheist/> (accessed on 17 October 2025).
135. Amnesty International. Repackaging Repression: The Cyber Security Act and the Continuing Lawfare Against Dissent in Bangladesh (Index: ASA 13/8332/2024). 2024. Available online: <https://www.amnesty.org/en/wp-content/uploads/2024/08/ASA1383322024ENGLISH.pdf> (accessed on 17 October 2025).
136. ICNL. Bangladesh's Cyber Security Act: A Guide for Civil Society, Media and the Public (Handbook). November 2024. Available online: <https://www.icnl.org/wp-content/uploads/Bangladesh-CSA-Handbook-Nov-2024.pdf> (accessed on 17 October 2025).
137. Supan, Q.M.H. *Review of Proposed Cyber Security Rules, 2024*; Position Paper; Transparency International Bangladesh: Dhaka, Bangladesh, 2024. Available online: <https://www.ti-bangladesh.org/upload/files/position-paper/2024/pcsr/Review-of-proposed-Cyber-Security-Rules-2024-En.pdf> (accessed on 17 October 2025).
138. Ehsan, S.B.; Saquib, M.N. Balancing cybersecurity and individual rights: A critical analysis of Bangladesh's Cyber Security Act 2023. *J. Creat. Writ.* **2024**, *8*, 81–93. [CrossRef]
139. Daily Star. Govt Repeals Cyber Security Act; New Cyber Security Ordinance Issued. Tech & Startup Desk. *The Daily Star*, 22 May 2025. Available online: <https://www.thedailystar.net/tech-startup/news/govt-repeals-cyber-security-act-new-cyber-security-ordinance-issued-3900681> (accessed on 17 October 2025).
140. FireEye. *M-Trends 2017: A View from the Front Lines*; FireEye: Milpitas, CA, USA, 2017. Available online: <https://fiswg.research.ucf.edu/Documents/PDF/Mandiant%20State%20of%20the%20Hack%20Overview%20of%20Recent%20Cyber%20Activity%20April%202017.pdf> (accessed on 17 October 2025).
141. SWIFT. Three Years on from Bangladesh: Tackling the Adversaries. SWIFT ISAC Report. April 2019. Available online: <https://www.swift.com/swift-resource/210491/download?language=en> (accessed on 17 October 2025).
142. Jugantor. 64 Individuals and Organizations Accused in the Bangladesh Bank Reserve Theft Case [Original Article in Bangla]. 18 June 2026. Available online: <https://www.jugantor.com/tp-firstpage/1115197> (accessed on 20 June 2026).
143. Bangladesh Bank. *Cybersecurity Framework 1.0*; Bangladesh Bank: Dhaka, Bangladesh, 2025.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.