Journal of Business and Economics, ISSN 2155-7950, USA
August 2024, Volume 15, No. 8, pp. 405-421
DOI: 10.15341/jbe(2155-7950)/08.15.2024/001

http://www.academicstar.us

Cyber Risk Management in Financial Institutions: Before and After the Bangladesh Bank Heist

Tanzina Sultana
(School of Business and Technology, Emporia State University, USA)

Abstract: The cyber heist of the Central Bank of Bangladesh in February 2016, which led to an $81 million loss, marks a significant event in the history of financial institution (FI) cyber-attacks. This paper examines the cyber risk management landscape within FIs before and after this landmark heist. It underscores the wake-up call to the international banking community, highlighting the vital need for robust cyber risk management frameworks to combat such sophisticated threats. The incident not only unveiled the shortcomings in the cybersecurity measures of a central bank but also demonstrated the extensive consequences of such breaches on the broader financial system. Our study analyzes the changes in risk management practices pre- and post-heist, emphasizing the enhancement of security protocols, employee training, incident response strategies, and the adoption of frameworks such as the NIST Cybersecurity Framework. By exploring this particular case, we aim to provide insights into the critical importance of managing cyber risks and to offer recommendations for strengthening the resilience of financial institutions against evolving cyber threats.

Key words: Bangladesh Bank Heist, cyber risk management, cybersecurity, banking sector resilience, SWIFT network

JEL code: M1

1. Introduction

The event that transpired in February 2016 when the Central Bank of Bangladesh was targeted in an $81 million cyber heist has been the most dramatic demonstration so far of the impact on international financial institutions (FIs) caused by a cyber-attack. The case is known as one of the most notable heists when attackers installed malware in the bank's computer systems to issue a series of SWIFT messages, which resulted in financial losses totaling $81 million from the Central Bank of Bangladesh (Karim & Hossain, 2021; Mazumder & Sobhan, 2020; Zafarullah & Haque, 2023; Mazumder & Hossain, 2023). This has led to increased scrutiny over the resilience of the banking systems and their preparedness against cyber-attacks. It is important to understand the distinction between the various types of FIs. The case of the Bangladesh heist demonstrated that an attack on a central bank can create a ricochet effect on the commercial banks within the country (Stoddart, 2022) As the central bank controls monetary policy and regulations, it was able to instruct changes to the value of currency to lessen the blow of the attack. This was done by the central bank submitting special treasury bonds to the

Tanzina Sultana, MBA and MSIT, School of Business and Technology, Emporia State University; research areas: cybersecurity, information technology and project management. E-mail: tsultana@g.emporia.edu.

commercial banks within Bangladesh with a reduced rate of interest to reduce availability of money (Van et al., 2022; He et al., 2022; Leombroni et al., 2021) The knock-on effect between the cyber-attack at a central bank and changes in the value of currency has not been seen in any other case, and this was a scenario that targeted an attack on the system and was not a goal of theft. In the current era, cyber risk has become an integral area of risk management, including financial and non-financial firms with an increased dependency on information technology (Eisenbach et al., 2022; Ros, 2020; George et al., 2024).

The importance of risk management for FIs facing an uncertain future in financial markets, and the Bangladesh heist is a prime example of an extreme uncertain event imposed on an FI (Afrin et al., 2020; Pollmeier et al., 2023). This demonstrates an urgency for research into how cyber risk is affecting global FIs, the distinctive risk identification of an attack on IT systems, and assessing the extreme nature of high-consequence, low probability events that cyber-attacks may present. The heist has shown the evolving nature of cyber-attacks from hackers to petty theft to what is now a sophisticated method, which has characteristics of being state-sponsored given the size of the money involved and the attempt to alter currency, which is a less trackable method of theft.

1.1 Background of the Bangladesh Bank Heist

In February 2016, unknown hackers breached the Bangladesh Bank's systems and issued over three dozen requests to the Federal Reserve Bank of New York to transfer funds from the bank's account to accounts in the Philippines and Sri Lanka. The total amount that the hackers made off with was roughly around $81 million (Sijan et al., 2022; Liu, 2021; Karim & Hasan, 2021). While most of the requests were rejected, around $20 million got routed to a fraudulent non-government organization based in the Philippines and then laundered through several casinos. If not for a simple spelling error, the total loss would have been around $1 billion (Jabar & Jesperson, 2024; Suh, 2023). This heist has been noted as one of the largest known bank heists in history.

The hackers were only stopped because the first transfer to the NGO was rejected due to the receiving accounts being misspelled. The hackers misspelled "foundation" in the NGO's name as "fandation", which caused a routing bank, Deutsche Bank, to seek clarification from the Bangladesh central bank, which then stopped the transactions. This already shows that, with the right moves, the hackers could have potentially swindled $950 million. Figure 1 (Abu Bakar et al., 2008) shows that the Lazarus group, a rumored North Korean state-sponsored Advanced Persistent Threat (APT) entity, targeted the Central Bank of Bangladesh. They used a range of techniques, including spear-phishing to gain initial access, SWIFT-IDRIDEX malware to target financial transactions, MACKTRUCK backdoor to sustain unauthorized access, and a counterfeit TLS protocol to conceal their malicious activities. The chosen victim highlights the strategic planning involved in the attack, with the aim of disrupting a vital national economic cornerstone (Lehto, 2022; Mott et al., 2023). This model provides insights into the attacker's identity, the techniques employed, and the broader implications for cybersecurity in the financial domain.

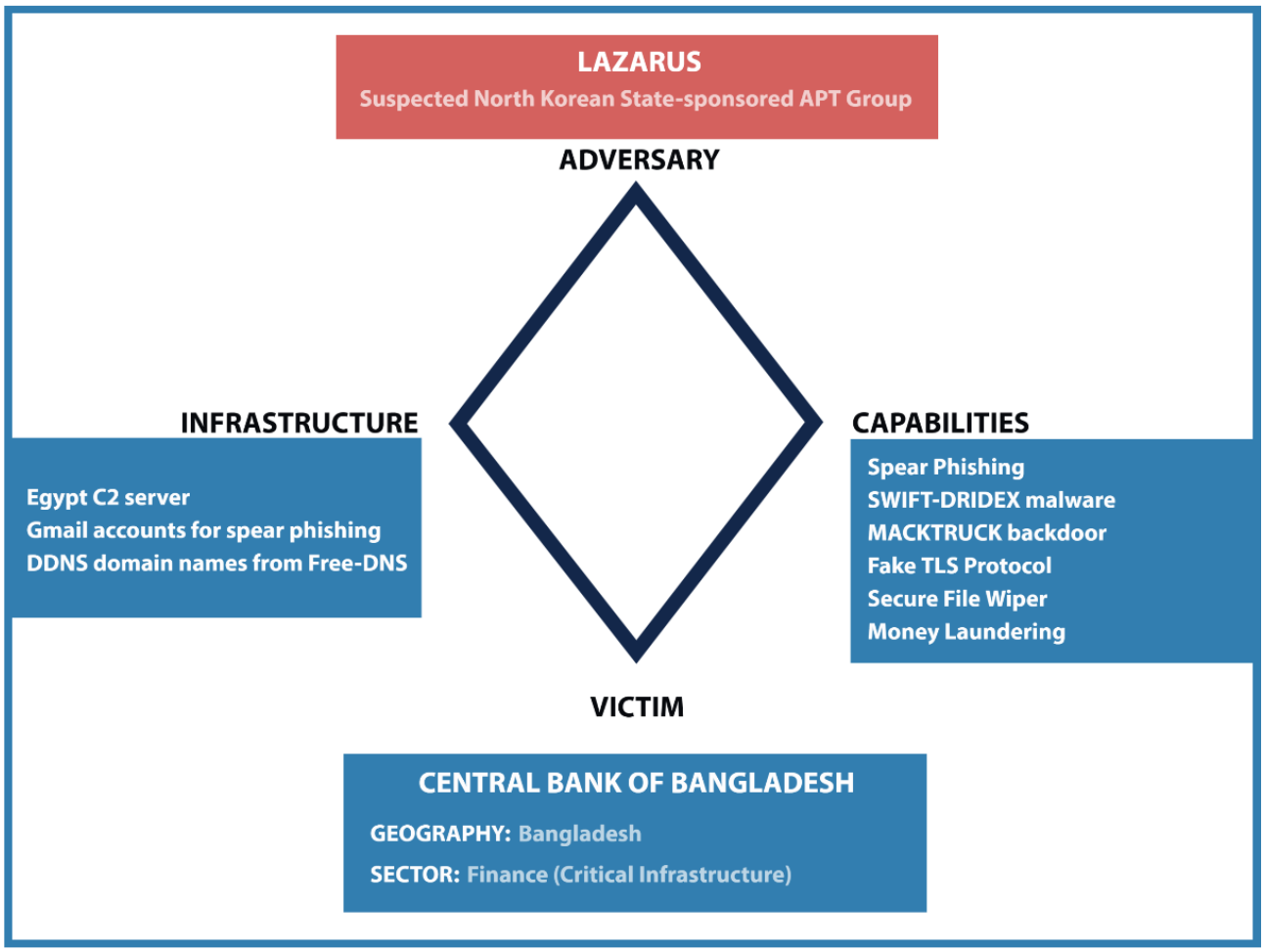

Figure 1 The Diamond Model Analysis of the Cyber Heist at Bangladesh Bank

Source: Abu Bakar et al., 2008

1.2 Importance of Cyber Risk Management in Financial Institutions

Cyber risk, as seen in the case of the Bangladesh bank heist, can have serious implications for any financial institution. This heist has shown the world the extent of financial loss a central bank can incur due to a cyber-attack (Mazumder & Sobhan, 2020; Hossain et al., 2023). At present, most of the top management of any financial institution has limited knowledge of cyber risks and threats, and they do not make informed decisions, especially on IT investments (Varga et al., 2021; Armenia et al., 2021). The need is to increase the level of awareness regarding the potential impacts that IT failures and security breaches can have on financial institutions and the financial system (Uddin et al., 2020; Marcu, 2021). IT specialists charged with implementing systems are not well linked with the business and risk management areas of financial institutions (Javaid et al., 2022). This leads to sub-optimal IT investment decisions and limits the ability of IT staff to properly target the areas of highest risk (Modelling the risk of IT investment decision-making in financial institutions, 2009). It has been found that cyber risk is best managed when decision-makers and influencers have a good understanding of the risk positions and can make well-informed decisions on the desired risk posture (Hart et al., 2020). In recent times, there have been lots of regulations coming up that require the board members to be accountable for the safety of customer data and for data breaches and their impacts. This will require the board members to have a good understanding of

the various cyber risks and threats and their possible impacts on financial institutions.

Financial institutions provide the backbone to any economy in the world (Abdulhakeem & Hu, 2021; Xu et al., 2021; Park and Kim, 2020; Eggers, 2020; Maiti et al., 2022). Without a sound financial system, no country can survive and sustain this globe. Over the past few centuries, the banking sector has evolved into the most trustworthy and reliable sector of any economy. With globalization and increasing use of technology, the face of the banking sector has changed tremendously (Chakravaram et al., 2021). More and more innovative products introduced by financial institutions have simplified our day-to-day banking needs. From storing customer data to its various transactions, everything has been digitized (Kamalaldin et al., 2020; Akter et al., 2022; Mhlanga, 2023; Filotto et al., 2021). This digitization has made our lives simple and easy, but at the same time, it has exposed the data to various risks.

1.3 Purpose of the Study

The importance of this heist to the world is understanding that the malware used in the attack was specifically targeted for the SWIFT Alliance Access software, the method through which the Bangladesh bank was able to connect to the Federal Reserve Bank (Hossain et al.). The malware was programmed to obtain detailed information about the payment systems and create fraudulent transfer orders (Karim & Hasan, 2021). If the malware was not mistakenly detected in a random check by a system operator, it could have potentially made fraudulent orders on banks' payments to cause an even bigger financial loss (Nicholls et al., 2021). This raises a huge concern for all financial institutions using the SWIFT network, as it shows their vulnerability to hackers. The fact that this specific heist was against a central bank as well makes it even more worrisome for financial institutions, as they are the supposed guardians of monetary and economic stability (Park, 2021; FATOKI, 2023; Jalkebro & Vlcek, 2023; Olivier, 2021; Hwang, 2020). It shows that if a central bank such as the Bangladesh Bank can be a victim of a cyber-attack, then any other financial institution is at great risk. This makes it essential that financial institutions recognize the potential financial loss they can endure through cyber-attacks and understand the importance of managing and mitigating the risk. This is the purpose of the study, to gain an understanding of cyber risk management and its significance in present day for financial institutions through an event-related case study. An event-related case study of this recent cyber-attack on the Bangladesh Bank using detailed information surrounding the attack would be an effective way to understand the importance of cyber risk management for financial institutions today.

What do people really know about the Bangladesh Bank heist? It was an event that shocked the finance sector when the Bangladesh Bank lost $81 million in February 2016. It is considered to be one of the biggest cyber heists in history. The funds were stolen from Bangladesh central bank’s account with the Federal Reserve in New York using fraudulent SWIFT messages. However, only 5 of the 35 fake orders to transfer money, totaling $101 million, were successful. The hackers attempted to steal $951 million from the Bangladesh Bank’s account, but all the unauthorized transactions were blocked except for the $81 million. If it were not for a simple spelling error, the cyber heist would have been about a 1-billion-dollar loss for Bangladesh. But why is this event of any importance to financial institutions around the world?

2. Pre-Heist Cyber Risk Management Practices

It is widely understood throughout various industries that effective risk management starts with (i.e., is wholly dependent upon) an organization’s understanding and identification of its resources and the threats that it

faces (Hubbard, 2020; Hillson & Simon, 2020; Landoll, 2021; Alzoubi, 2022; Lee, 2020; Health Organization, 2023). For the cyber security industry, this is achieved through the identification of information assets, and an understanding of what adverse events can affect the asset (Corallo et al., 2020; Progoulakis et al., 2021; González-Granadillo et al., 2021). Financial institutions have an abundance of information resources and varying degrees of knowledge on how these resources intermingle and their potential adverse impacts (Rahman et al., 2024) However, the risk assessment function was not widely performed using information security experts and security measures for this specific task are usually basic (Landoll, 2021; Shin & Lowry, 2020). One of the interview subjects for this study, who is currently working in a leading capital markets data management company, explained that they have highly redundant systems and data warehousing (Cuzzocrea et al., 2020; Bimonte et al., 2022), but that they "have never seen a security measure designed to identify where we store data and what data is important to us" (Thompson & Warzel, 2022; Seth et al., 2022). With no specific security measures being taken to identify the data locations and a lack of expertise in the assessment task, it is fair to say that risk assessment in most financial institutions (and other industries) holds potential for significant improvement.

Heist Cyber Risk Management Practices Until the Bangladesh heist, many (i.e., most) banks lacked specific, formal, and enterprise-wide cyber security risk management programs with documented risk management strategies. Often, banks also do not have thorough understanding of their critical networks and data assets, know what level of risk they currently face, or what could be the potential impact and losses (Campiglio et al., 2023; Ellis et al., 2022; Murinde et al., 2022). As a result, it is difficult for management to justify the expense of additional security measures when they cannot quantify the loss that they are protecting against (Hossain, Hasan, Islam, Sultana, Sadil, & Ali, 2024). The identification and assessment of cyber risk thus far have been weak points for the financial sector. The following is a list of common risk management practices and how they were being performed in most financial institutions before the heist:

2.1 Risk Assessment and Identification

This process, which purely assesses the likelihood and impact on threats to assets, is not directly applicable to identifying unknown risk, as unknown risk by its nature cannot be measured (Dekker & Alevizos, 2024; Hubbard & Seiersen, 2023; Pascarella et al., 2021). Nonetheless, the identification of threats and assessment of their impact is an essential step in identifying where there is unknown risk, as many adverse effects of unknown risk are often caused by the occurrence of a threat that was not foreseen (Zografopoulos et al., 2021; Ganin et al., 2020). An example of this was the global ransomware attack in 2017, where many organizations had not foreseen the threat of a ransomware attack and were caught out by it, causing a high level of impact on those that were infected (Pagán & Elleithy, 2021). To identify the level of known risk, a formalized risk assessment methodology should be employed across the entire organization. Often, this is done by first identifying the assets that the organization has, then looking at the threats to those assets and identifying the vulnerabilities that when exploited by a threat, will cause an impact on the organization (Alshurideh et al., 2022; Settembre-Blundo et al., 2021). The assessment is in the form of identifying the likelihood of the threat occurring and the impact it would have if it did (El Baz & Ruel, 2021). This forms the basis for a later calculation of the level of risk. The identified risks should be documented in a risk register to ensure that the level of risk is updated should the occurrence of the threat or the vulnerability change. The risk assessment process in risk management aims to identify and assess the level of risk faced by the institution (Landoll, 2021; Van Greuning & Bratanovic, 2020; Hubbard, 2020; Ullah et al., 2021). There are mainly two types of risk: the known risk, where the impact and probably the likelihood of occurrence

can be estimated, and the unknown risk, where these cannot be measured. The known risk can be simply assessed using the formula:

$$Risk = Impact\ x\ Likelihood$$

2.2 Security Controls and Measures

Security controls and measures taken by Dhaka Central Bank were ineffective before the incident. Systems to prevent unauthorized transactions were not in place (Benazir, 2022; Milon & Zafarullah, 2024; Goodell et al., 2024; Uddin et al., 2020; Meraj et al., 2022). It was reported by FireEye that the central bank was using free malware to detect and remove malware from the systems, which had not been updated for the last 2 years. Symantec claimed that the malware was initiated by basic access credentials and then gaining in-depth knowledge of workings and operations, which caused a huge loss (Kleymenov & Thabet, 2022; Ruiz, 2021; Makrakis et al., 2021). The malware was used to exploit the network in such a way that transactions through the SWIFT network sounded like normal routine activity (FATOKI, 2023). But remember, the network where transactions were initiated is different from the network exploited by the attackers (Attkan & Ranga, 2022). The only beneficial security step taken by the central bank was that they were using a second-hand network to mimic the original SWIFT network, which saved the second part of the instructed transactions (Cirolia et al., 2022). Also, logical access control (Egala et al., 2021; Liu et al., 2020; Sookhak et al., 2021; Karo et al., 2023) was not in place. It was concluded by various security firms that the compromise was initiated by the access of credentials for the first two systems. The user IDs of the normal staff were compromised, who had initial access to the Bangladesh Bank systems, and the second set of access credentials belonged to the people who were directly involved in the SWIFT payment process (Hossain et al.; Karim & Hasan, 2021; Sayduzzaman et al., 2021). Compiling these 2 sets of access credentials caused the initiation of the transactions instructed by the attackers. Lack of separation of duties and irregular access level audits at Bangladesh Bank resulted in users having more access than necessary. An unusual printer was found to be a network gateway to the new printer server, which, upon investigation, led to the discovery of malware on the server.

2.3 Employee Training and Awareness

Training employees about relevant cyber threats and how they can prioritize their day-to-day accountabilities with best security practices is critical (Uchendu et al., 2021; Onwubiko & Ouazzane, 2022; Franchina et al., 2021; Safitra et al., 2023; Luo et al., 2023). If an institution can get employees to comprehend the significance of regular security assessments, following proper security controls, and being aware of their surroundings, the battle is more than half won (Sánchez-Zas et al., 2023). However, effective training is always easier said than done. The banking industry is always overloaded with mandatory compliance training, product training, and various other trainings aimed at improving customer service, knowledge, and efficiency (Ogunode et al., 2023; Kayode-Ajala2023; Ul Haque, 2023; Drougkas, 2024). Finding time to fit in cybersecurity training and awareness can be a difficult task. Often, institutions will resort to annual or bi-annual security training seminars conducted by internal or external security professionals (Mott et al., 2023). While this is certainly better than nothing, grouping an entire year's worth of cybersecurity education into a 1–2-hour seminar tends to be ineffective and short-lived. Employees at all levels and in all departments should have access to frequent microlearning modules that cover various security threats and best practices (Le et al., 2023). These learning modules should be short and interactive and should be followed by regular simulated phishing exercises to keep security best practices fresh in the minds of employees (Oruc et al., 2024). Financial institutions can truly maximize the effectiveness of their training and awareness

programs by cultivating a security culture throughout the organization (Masuduzzaman & Hussain, 2012; Bandari, 2023). This has been pointed out as an area where the Bangladesh Bank failed miserably. In an atmosphere with a strong security culture, security is a priority and is not viewed as an obstacle to productivity. It is integrated into daily tasks and decisions and is in everyone's mind. Employees are aware of security risks and are comfortable discussing security concerns with colleagues and management (Triplett, 2022; McDonald et al., 2021). Creating a security culture takes time and dedication, but it has been proven to change employee behavior and minimize security risks (Georgiadou et al., 2022; Sharma & Aparicio, 2022). A security culture can be advanced through various methods, such as security awareness posters and bulletin boards, appointing security "champions" in each department, and incorporating security discussions into regular meetings and other communications with employees.

2.4 Incident Response and Recovery Plans

According to the survey conducted prior to the heist, not even one of the 38 respondents believed that it was very likely for a cyber incident to occur against the central bank (Ekong Eyo, 2023). The incident has induced most financial institutions to reconsider their risk of exposure to cyber threats (Pollmeier et al., 2023). Despite the occurrence of the heist, many respondents still agreed that such incidents were still somewhat unlikely at the time for their own institution (Moosa et al., 2023). While there has been a rise in perceived likelihood of a cyber incident against central banks (Eisenbach et al., 2022; Soderberg et al., 2022; Allen et al., 2022), the actual risk assessment against specific threats from central bank networks has not changed significantly. This logic is valid when considering that the unknown threat actor was able to exploit vulnerabilities in the central bank's connections to the SWIFT network to send instructions to transfer large sums of money to fraudulent accounts in a foreign country. Identification of risks has been worse overall, with 4 respondents claiming their institution had identified any new cyber-related risks since the occurrence of the heist and only 3 respondents claimed identification of specific new threats against central banks (Siderius, 2023). A lack of improvement in identification of cyber risks most likely mirrors the fact that identification of the specific tactics, techniques, and procedures used by threat actors in the recent incidents is difficult due to scarcity of intelligence information to which only a select few cybersecurity firms and analysts have access (Cremer et al., 2022; Wanof, 2023; Chauhan et al., 2022). New techniques and information regarding adversary methods for central banks would not commonly be publicized to prevent further attacks. This directly contradicts one of the central bank’s main defenses that led 3 respondents to admit it's possible that the recent incidents caused an increase in security controls on systems directly involved with fund transfers (Piroska & Mérő, 2021).

3. Post-Heist Changes in Cyber Risk Management

As a direct result of the heist, Bangladesh Bank has substantially changed its cyber risk management processes and systems (Mazumder & Hossain, 2023; Sijan et al., 2022; Sikder & Islam, 2023). This can be broken down into five main areas. The first area sits within their risk assessment function, where they have implemented a monthly cyber security risk assessment. This increased cadence allows them to better understand the risks that the bank faces and provides a feedback loop from the assessment into the rest of the cyber risk management function. They have predominantly been using the NIST cybersecurity framework to conduct these assessments. This is a considerable enhancement from the annual risk assessment process that was in place prior to the heist. In particular, the forms of intelligence used to inform the risk assessment have been expanded to include open-source

intelligence and a service provided by the government (Ghioni et al., 2023). Step changes are also being made to formalize the risk assessment process so that identified risks can be tracked and reported on to ensure that they are being mitigated or accepted with a risk treatment plan in place. Finally, to monitor the performance of the risk assessment function, KPIs and KRIs are being developed with the goal of being able to detect future deviation from normal performance.

3.1 Strengthening Risk Assessment and Identification

Fallacious risk assessment and identification predated the breach, and it stands as one of the main organizational factors behind why the hackers were successful in their compromise (Pearson, 2021; Spafford et al., 2023; Becote, 2023). The group didn't have a formalized risk assessment methodology and risk analysis process, despite being introduced in the COSO ERM framework, Australia/New Zealand risk management standard, and the ISO31000:2009 risk management principles and guidelines (Landoll, 2021; Settembre-Blundo et al., 2021). There was no formal understanding of the types of risks the bank faces and how those risks relate to the potential impact on business objectives. The group did not consider political or geopolitical changes in other countries (Chu et al., 2023; Wang et al., 2023; Flouros et al., 2022). In this case, it was the change in relations between Iran and other western countries (Eskandari et al., 2020). This resulted in no change in the risk appetite for transacting with Iranian companies, which would go on to bear a substantial impact on the group. Without a sustainable risk analysis process, the group ended up making high-level risk decisions without understanding the potential impact on specific business objectives. The shift of the switch installation project to the SWIFT environment is an example of this, as the group did not consider the potential risk to their previous objectives of cost reduction and improved service speed (Mani & Goniewicz, 2023). Due to the hackers' initial focus on Bangladesh Bank's move to real-time gross settlement (RTEGS), senior management made this decision without conducting a risk analysis, which would have a significant impact on the company. The oversight also resulted in minimal IT and security spending.

3.2 Enhancing Security Controls and Measures

Immediate enhancement of security controls and measures is the obvious action to take following a major cyber-security incident, and central bank cyber-security experts were quick to point this out in reference to the Bangladesh case. First and foremost, the Bangladesh incident has illustrated that prevention is better than cure. At face value, the SWIFT software was not the only component of the Bangladesh Bank connection to the international payments system that had vulnerabilities (Shalabi et al., 2023). The culprits took advantage of second-hand security controls surrounding the Bangladesh Bank's connection to the SWIFT network. Specific details have not been disclosed; however, it is known that the culprits submitted a total of 35 fraudulent payment instructions to the Federal Reserve Bank of New York, of which 5 succeeded. If the SWIFT software at the central bank had been better protected, and if stronger security controls had been put in place to authorize and verify each payment instruction, it is less likely that the transfer orders would have been processed. The Bangladesh Bank incident has shown that hackers are very resourceful and will take the path of least resistance to achieve their goals. One observed modus operandi of cyber-criminals over recent years has been to target banks and other financial institutions through their connections to third-party service providers (Deb, 2020). This was the case in the Carbanak attacks, which netted an estimated $1 billion in losses from over 100 financial institutions (Noor et al., 2023). SWIFT has been too quick to highlight that the Bangladesh case is part of a wider and highly adaptive campaign to target banks. In securing their own organizations, other banks need to take heed of the wider

implications of this and consider third-party service providers as extensions of their own organizations that are also at risk from cyber-attacks (Liao et al., 2022).

3.3 Improving Employee Training and Awareness

There were three main issues with the bank's security system. Firstly, there were an unusually large number of connected endpoints. Secondly, there was no firewall in place. Thirdly, there was no segregation between the SWIFT systems and the rest of the bank's networks (Ali et al., 2022; Rabiul Hasan, 2024; Golightly et al., 2023). All three of these issues resulted from a lack of adequate security controls but may have been avoided had employees been trained with a security mindset. If there had been awareness that an unusually large number of endpoints and a lack of firewalls are security risks, they may have been caught before allowing the attackers to persist for several weeks. These are issues that likely should have been escalated to the management and risk assessment of the systems (Aven & Zio, 2021). In doing this, we expect that the security requirements for the systems involved will be increased. After the heist, the bank appointed FireEye's Mandiant incident response team to conduct a forensic investigation into the bank's security incident. Attackers are abusing the SWIFT network to send fraudulent messages to other financial institutions seeking to transfer nearly $1 billion from the bank's account at the Federal Reserve Bank of New York. The fraud was partially successful, resulting in the transfer of $81 million to bank accounts in the Philippines. Fortunately, with the assistance of the New York Fed, most of the payment orders were blocked, but approximately $20 million made its way to the Philippines. The investigation revealed several issues with the bank's security. Security experts at Fright & Sullivan believe that these findings are indicative of the security posture at most large financial institutions.

3.4 Updating Incident Response and Recovery Plans

The Bangladesh Bank heist prompted financial regulatory authorities and central banks worldwide to review their cybersecurity risk management and incident response plans (Stanikzai & Shah, 2021; Sikder & Islam, 2023; Kafi & Akter, 2023). Institutions are advised to apply general disaster recovery practices to cyber-attack scenarios (Salvi et al., 2022). Central banks should simulate the attack to manage its impact on confidence and foreign reserve currency. Communication with all stakeholders is essential to assess the impact and possible contingency measures (Ramirez, 2024). The US Federal Reserve provides an excellent example of an internal escalation system for crisis scenarios with a series of playbooks to coordinate with the US Treasury Department (Buehler et al., 2020). There is a wide variation in the level of sophistication and coverage of incident response and recovery planning across financial institutions. However, before the heist, incident response planning by central banks was often inadequate, with many lacking formal and tested procedures. In contrast, recovery plans for system outages followed by data integrity loss were often quite detailed and well documented. This difference reflects the fact that recovery from a cyber-attack was often seen as an IT problem rather than a central bank-wide issue and thus would be dealt with by the IT department concerned using internal resources (Hossain, Sultana, Zabeen, & Sarpong, 2024).

3.5 Collaborating With External Agencies and Institutions

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a cooperative that belongs to all its international member financial institutions (Qin & Mogos, 2022; Campbell, 2023; Irkliienko, 2023). Its mission is to facilitate the exchange of automated clearing house (ACH) transactions and the transfer of funds between businesses both internationally and domestically (Beltrán & Bär, 2022; Melito, 2020; Hefny et al., 2023).

After the security incidents in member banks, including the Bangladesh Central Bank and several commercial banks, SWIFT initiated an aggressive customer security program designed to combat the growing threat of cyber-attacks on SWIFT customers. A central pillar of the initiative is the sharing of cyber security information among all participants in the program (Jhanjhi et al., 2021). This includes details about specific security incidents, methods employed by attackers, and threat intelligence indicators. With the goal of enhancing cyber defenses throughout the entire SWIFT community, SWIFT will facilitate information sharing in a secure and private setting. The customer security program also includes tools designed to help banks improve their security posture, both locally and on the SWIFT network (Cipriani et al., 2023). By employing these tools, banks will be better equipped to identify and combat fraudulent use of their logical security credentials, as well as any resulting cyber incidents. The most powerful tool in the fight against global cyber-crime is effective collaboration among public, private, and international entities (Choi & Dulisse, 2023; Shakhbazian, 2021; Ruvin et al.2020; Ilbiz & Kaunert, 2023). As the sophistication of cyber-attacks increases, the scope of such criminal activity often extends beyond the borders of individual countries. In this environment, successful efforts to combat cyber-crime require the formation of alliances across various sectors. In the case of the Bangladesh Bank heist, a combination of cross-industry information sharing, and international diplomacy played a crucial role in identifying the attackers and preventing more incidents.

4. Lessons Learned and Future Directions

The Bangladesh Bank heist and subsequent cyberattacks on financial institutions worldwide serve as a cautionary tale against complacency and highlight the importance of managing cyber risks. The attack exploited vulnerabilities in SWIFT software due to the affected bank's lack of basic security measures. Institutions must stay abreast of emerging threats and advancements in security practices to prevent such oversights. The global banking system is interconnected, and an attack on one institution can quickly spread to others. The incident highlights the importance of robust payment verification processes and heightened security in correspondent banking, an area that has historically been overlooked in terms of compliance and security controls. ISO 27001 advises financial institutions to conduct regular risk assessments to manage cyber risks. Risk assessments should identify threats and vulnerabilities that could cause loss or damage to information. The results of these assessments help evaluate potential incidents and decide which actions to take to mitigate identified risks. This structured approach emphasizes a top-down, risk-based approach to information security, moving away from a controls-based ad hoc approach to mitigating risks. It should ultimately direct investment to where it is most needed — managing information security risks. ISO 27001 advises regular risk assessments to manage cyber risks. These assessments identify threats and vulnerabilities that could cause information loss or damage. The results help evaluate potential incidents and decide on actions to mitigate risks. Risk assessments should be ongoing and reviewed when significant changes occur. This approach is a top-down, risk-based approach to information security, directing investment to manage information security risks. It applies to financial services and outsourcing providers. The standard also applies to information assets that are accessed, processed, communicated, or stored by other parties on behalf of the organization. This includes cloud service providers and third-party vendors. These parties must adhere to the same security controls and risk assessment processes to ensure the overall security of the organization’s information assets. Failure to do so can result in potential vulnerabilities and weak links in the organization’s cyber risk management framework.

5. Recommendations for Financial Institutions

Financial institutions face challenges due to changing customer expectations, regulations, and cybersecurity threats. They need innovative approaches, robust risk management frameworks, and cutting-edge technology solutions to address these. Blockchain can help improve cybersecurity and risk management efforts, reducing the risk of fraud and data breaches (Hossain et al., 2024). Third-party service providers must undergo a similar risk assessment, and higher-risk services require a dedicated payment environment. Financial institutions can remain agile and successful by proactively identifying emerging trends and devising comprehensive strategies.

6. Conclusions

The Bangladesh Bank Heist of 2016 reminds us of the increasing threat of cyberattacks on financial institutions worldwide. This highly sophisticated attack involved infiltrating the bank's computer systems, using social engineering tactics, and receiving insider help. The attack resulted in a loss of $81 million, significantly impacting Bangladesh's economy and banking system. Financial institutions must take proactive measures to prevent similar incidents in the future. These measures include implementing two-factor authentication, conducting regular security audits, being vigilant against insider threats, and providing cybersecurity awareness training to employees. They must also stay up-to-date with the latest cybersecurity trends and technologies to ensure they are adequately protected. Financial institutions must have incident response plans in place in case of a cyberattack. These plans should include protocols for detecting and containing a breach, notifying relevant parties, and recovering from the attack. Financial institutions must protect their systems, data, and customers by implementing best practices in cybersecurity, conducting regular security audits, and providing employee training. By taking proactive measures, financial institutions can minimize the risk of a successful cyberattack and protect themselves from significant financial and reputational damage.

References

Abdulhakeem S. A. and Hu Q. (2021). Powered by Blockchain technology, DeFi (Decentralized Finance) strives to increase financial inclusion of the unbanked by reshaping the world financial …. Modern Economy. scirp.org

Afrin S., Sehreen F., Polas M. R. H. and Sharin R. (2020). "Corporate Social Responsibility (CSR) practices of financial institution in Bangladesh: The case of United Commercial Bank", *Journal of Sustainable Tourism and Entrepreneurship*, Vol. 2, No. 2, pp. 69-82.

Akter S., Michael K., Uddin M. R., McCarthy G. and Rahman M. (2022). "Transforming business using digital innovations: The application of AI, blockchain, cloud and data analytics", *Annals of Operations Research*, pp. 1-33.

Al Mamun A., Ibrahim J. B. and Mostofa S. M. (2021). "Cyber security awareness in Bangladesh: An overview of challenges and strategies", *Int. J. Comp. Sci. Informat. Technol. Res*, Vol. 9, pp. 88-94.

Ali S. M., Hoq S. M. N., Bari A. B. M. M., Kabir G. and Paul S. K. (2022). "Evaluating factors contributing to the failure of information system in the banking industry", *Plos One*.

Allen F., Gu X. and Jagtiani J. (2022). "Fintech, cryptocurrencies, and CBDC: Financial structural transformation in China", *Journal of International Money and Finance*.

Alshurideh M. T., Alzoubi H. M. and Ghazal T. M. (2022). "Risk management model for telecom enterprises based on variables (RM, SO, RC, SI) with nature, sense and positive psychology hypothesis", *Journal for ReAttach Therapy and Developmental Diversities*, Vol. 5, No. 2s, pp. 152-162.

Alzoubi H. M. (2022). "BIM as a tool to optimize and manage project risk management", *International Journal of Mechanical Engineering*.

Armenia S., Angelini M., Nonino F., Palombi G. and Schlitzer M. F. (2021). "A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs", *Decision Support Systems*, Vol. 147, p. 113580.

Attkan A. and Ranga V. (2022). "Cyber-physical security for IoT networks: A comprehensive review on traditional, blockchain and artificial intelligence based key-security", *Complex & Intelligent Systems*.

Aven T. and Zio E. (2021). "Globalization and global risk: How risk analysis needs to be enhanced to be effective in confronting current threats", *Reliability Engineering & System Safety*.

Bandari V. (2023). "Enterprise data security measures: A comparative review of effectiveness and risks across different industries and organization types", *International Journal of Business Intelligence and Big Data Analytics*, Vol. 6, No. 1, pp. 1-11.

Bartram J., Corrales L., Davison A., Deere D., Drury D., Gordon B., Howard G., Rinehold A. and Stevens M. (2009). *Water Safety Plan Manual: Step-By-Step Risk Management for Drinking-Water Suppliers*, World Health Organization.

Becote B. (2023). "Defining a cyber operations performance framework via computational modeling", available online at: http://www.dsu.edu

Beltrán J. M. and Bär F. (2022). "The European Automated Clearing Association and the role of clearing and settlement mechanisms in Europe's evolving payments landscape", *Journal of Payments Strategy & Systems*.

Benazir N. S. (2022). "Control of fraud and unauthorized payments in the MFS industry: An exploratory study of bKash Limited", available online at: http://www.bracu.ac.bd.

Bimonte S., Gallinucci E., Marcel P. and Rizzi S. (2022). "Data variety, come as you are in multi-model data warehouses", Information Systems, available online at: http://www.unibo.it.

Buehler K., Conjeaud O., Giudici V., Samandari H., Serino L., Vettori M. and White O. et al. (2020). "Leadership in the time of coronavirus: COVID-19 response and implications for banks", *McKinsey Insights*, available online at: http://www.mckinsey.com.

Campbell A. (2023). "The cross-border interbank payment system: A case study in Chinese Economic Leadership", available online at: http://www.umass.edu.

Campiglio E., Daumas L., Monnin P. and von Jagow A. (2023). "Climate-related risks in financial assets", *Journal of Economic Surveys*, Vol. 37, No. 3, pp. 950-992.

Chakravaram V., Ratnakaram S., Vihari N. S. and Tatikonda N. (2021). "The role of technologies on banking and insurance sectors in the digitalization and globalization era — a select study", in: *Proceedings of International Conference on Recent Trends in Machine Learning*, IoT, Smart Cities and Applications: ICMISC 2020, Springer Singapore, pp. 145-156.

Chauhan V., Yadav R. and Choudhary V. (2022). "Adoption of electronic banking services in India: An extension of UTAUT2 model", *Journal of Financial Services Marketing*, pp. 1-14.

Choi J. and Dulisse B. (2023). "Techno-crime prevention: the role of the private sector and its partnerships with the public sector", in: *Handbook on Crime and Technology*.

Chu L. K., Doğan B., Ghosh S. and Shahbaz M. (2023). "The influence of shadow economy, environmental policies and geopolitical risk on renewable energy: A comparison of high-and middle-income countries", *Journal of Environmental Management*, Vol. 342, p. 118122.

Cipriani M., Goldberg L. S. and La Spada G. (2023). "Financial sanctions, SWIFT, and the architecture of the international payment system", *Journal of Economic Perspectives*, Vol. 37, No. 1, pp. 31-52.

Cirolia L. R., Hall S. and Nyamnjoh H. (2022). "Remittance micro-worlds and migrant infrastructure: Circulations, disruptions, and the movement of money", *Transactions of the Institute of British Geographers*, Vol. 47, No. 1, pp. 63-76.

Corallo A., Lazoi M. and Lezzi M. (2020). "Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts", *Computers in Industry*.

Cremer F., Sheehan B., Fortmann M., Kia A. N., Mullins M., Murphy F. and Materne S. (2022). "Cyber risk and cybersecurity: A systematic review of data availability", *The Geneva Papers on Risk and Insurance-Issues and Practice*, Vol. 47, No. 3, pp. 698-736.

Cuzzocrea A., Ferreira N. and Furtado P. (2020). "A rewrite/merge approach for supporting real-time data warehousing via lightweight data integration", *The Journal of Supercomputing*.

Deb D. (2020). "A critical analysis on cyber crimes and e-banking services available to resolve issues with reference to RBI's Role".

Dekker M. and Alevizos L. (2024). "A threat-intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision-making", *Security and Privacy*.

Drougkas E. (2024). "Communication gaps in current business processes and analyzing the interconnections between departments to ensure customer engagement and satisfaction".

Egala B. S., Pradhan A. K., Badarla V. and Mohanty S. P. (2021). "Fortified-chain: A blockchain-based framework for security and privacy-assured internet of medical things with effective access control", *IEEE Internet of Things Journal*, Vol. 8, No. 14, pp.

11717-11731.

Eggers F. (2020). “Masters of disasters? Challenges and opportunities for SMEs in times of crisis”, *Journal of business Research*.

Eisenbach T. M., Kovner A. and Lee M. J. (2022). “Cyber risk and the US financial system: A pre-mortem analysis”, *Journal of Financial Economics*.

Ekong Eyo U. (2023). “Impact of cyber-security on financial fraud in commercial banks in Nigeria: A case study of Zenith Banks in Abuja”, available online at: http://www.aust.edu.ng.

El Baz J. and Ruel S. (2021). “Can supply chain risk management practices mitigate the disruption impacts on supply chains' resilience and robustness? Evidence from an empirical survey in a COVID-19 outbreak era”, *International Journal of Production Economics*.

Ellis S., Sharma S. and Brzeszczyński J. (2022). “Systemic risk measures and regulatory challenges”, *Journal of Financial Stability*.

Eskandari S., Pourghasemi H. R. and Tiefenbacher J. P. (2020). “Relations of land cover, topography, and climate to fire occurrence in natural regions of Iran: Applying new data mining techniques for modeling and mapping fire danger”, *Forest Ecology and Management*, Vol. 473, p. 118338.

Fatoki J. O. (2023). “The influence of cyber security on financial fraud in the Nigerian banking industry”, *International Journal of Science and Research Archive*.

Filotto U., Caratelli M. and Fornezza F. (2021). “Shaping the digital transformation of the retail banking industry: Empirical evidence from Italy”, *European Management Journal*.

Flouros F., Pistikou V. and Plakandaras V. (2022). “Geopolitical risk as a determinant of renewable energy investments”, *Energies*.

Franchina L., Inzerilli G., Scatto E., Calabrese A., Lucariello A., Brutti G. and Roscioli P. (2021). “Passive and active training approaches for critical infrastructure protection”, *International Journal of Disaster Risk Reduction*, No. 63, p. 102461.

Ganin A. A., Quach P., Panwar M., Collier Z. A., Keisler J. M., Marchese D. and Linkov I. (2020). “Multicriteria decision framework for cybersecurity risk assessment and management”, *Risk Analysis*, Vol. 40, No. 1, pp. 183-199.

George A. S., Baskar T. and Srikaanth P. B. (2024). “Cyber threats to critical infrastructure: Assessing vulnerabilities across key sectors”, *Partners Universal International Innovation Journal*, Vol. 2, No. 1, pp. 51-75.

Georgiadou A., Mouzakitis S., Bounas K. and Askounis D. (2022). “A cyber-security culture framework for assessing organization readiness”, *Journal of Computer Information Systems*, Vol. 62, No. 3, pp. 452-462.

Ghioni R., Taddeo M. and Floridi L. (2023). “Open source intelligence and AI: A systematic review of the GELSI literature”, *AI & Society*.

Golightly L., Modesti P., Garcia R. and Chang V. (2023). “Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN”, *Cyber Security and Applications*.

González-Granadillo G., González-Zarzosa S. and Diaz R. (2021). “Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures”, *Sensors*.

Goodell G., Al-Nakib H. D. and Aste T. (2024). “Retail central bank digital currency: Motivations, opportunities, and mistakes”, arXiv preprint arXiv:2403.07070.

Hart S., Margheri A., Paci F. and Sassone V. (2020). “Riskio: A serious game for cyber security awareness and education”, *Computers & Security*.

He Z., Nagel S. and Song Z. (2022). “Treasury inconvenience yields during the COVID-19 crisis”, *Journal of Financial Economics*.

Hefny M. H. M., Helmy Y. and Abdelsalam M. (2023). “Open banking api framework to improve the online transaction between local banks in Egypt using blockchain technology”, *Journal of Advances in Information Technology*, Vol. 14, No. 4, pp. 729-740.

Hillson D. and Simon P. (2013). *Practical Project Risk Management: The ATOM Methodology*, Pm Network.

Hossain M. I., Hasan R., Islam M. J., Sultana T., Sadil S. and Ali M. W. (2024). “Strategic identification and selection of information systems projects”, *International Journal for Multidisciplinary Research*, Vol. 6, No. 1.

Hossain M. A., Sarker M. D. A., Hossain M. S., Shaon M. A. R., Hossain M. S., Rayhan, M. M. H. and Astudillo J. G. S. (n.d.). “Bangladesh Bank Money Heist: A concern of cybersecurity system of Bangladesh Bank and way forward”.

Hossain M. I., Steigner D. T., Hussain M. I. and Akther A. (2024). “Enhancing data integrity and traceability in industry cyber physical systems (ICPS) through blockchain technology: A comprehensive approach”, arXiv preprint arXiv:2405.04837.

Hossain M. I., Sultana T., Zabeen W. and Sarpong A. F. (2024). “Transformational outsourcing in IT project management”, arXiv preprint arXiv:2405.01544.

Hubbard D. W. and Seiersen R. (2023). “How to measure anything in cybersecurity risk”, doi: 10.1002/9781119162315, 111-112.

Hubbard D. W. (2020). *The Failure of Risk Management: Why It's Broken and How to Fix It*.

Hwang T. (2020). *Subprime Attention Crisis: Advertising And the Time Bomb at the Heart of the Internet*, New York, NY: Farrar, Strauss, and Giroux.

Ilbiz E. and Kaunert C. (2023). "Cybercrime, public-private partnership and Europol", in: *The Sharing Economy for Tackling Cybercrime*.

Irkliienko O. (2023). *Financial Instruments in Facilitating International Trade: On The Basis of Privat Bank*.

Jabar M. and Jesperson S. (2024). "Analysis of labour migrants' vulnerabilities to trafficking in persons and labour exploitation in the Philippines", available online at: http://www.cdn.ngo.

Jalkebro R. and Vlcek W. (2023). "The future of criminal finance: 'bin Ladens' and the cashless society", in: *Organized Crime, Financial Crime, and Criminal Justice*, Routledge, pp. 104-121.

Javaid M., Haleem A., Singh R. P., Suman R. and Khan S. (2022). "A review of Blockchain Technology applications for financial services", *Bench Council Transactions on Benchmarks, Standards and Evaluations*, Vol. 2, No. 3, p. 100073.

Jhanjhi N. Z., Humayun M. and Almuayqil S. N. (2021). "Cyber security and privacy issues in industrial internet of things", *Computer Systems Science & Engineering*, Vol. 37, No. 3.

Kafi M. A. and Akter N. (2023). "Securing financial information in the digital realm: Case studies in cybersecurity for accounting data protection", *American Journal of Trade and Policy*.

Kamalaldin A., Linde L., Sjödin D. and Parida V. (2020). "Transforming provider-customer relationships in digital servitization: A relational view on digitalization", *Industrial Marketing Management*, Vol. 89, pp. 306-325.

Karim M. R. and Hossain M. A. (2021). "Fraudulent financial reporting in the banking sector of Bangladesh: A prediction", *International Journal of Management, Accounting & Economics*, Vol. 8, No. 2.

Karim Y. and Hasan R. (2021). "Taming the digital bandits: An analysis of digital bank heists and a system for detecting fake messages in electronic funds transfer", *National Cyber Summit (NCS) Research Track 2020*.

Karo M., Yeredor A. and Lapidot I. (2023). "Compact time-domain representation for logical access spoofed audio", *IEEE/ACM Transactions on Audio, Speech, and Language Processing*.

Kayode-Ajala O. (2023). "Applications of cyber threat intelligence (CTI) in financial institutions and challenges in its adoption", *Applied Research in Artificial Intelligence and Cloud Computing*, Vol. 6, No. 8, pp. 1-21.

Kleymenov A. and Thabet A. (2022). "Mastering malware analysis: A malware analyst's practical guide to combating malicious software, APT, cybercrime, and IoT attacks", available online at: http://www.ttgtmedia.com.

Landoll D. (2010). *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*, Boca Raton, FL: CRC Press.

Le D., Matsuda C., Pena S., Platou I. and Olsen T. (2023). "Effective cybersecurity training using microlearning and the drip concept: A case study of a large regional hospital", available online at: http://www.drake.edu.

Lee I. (2020). Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. Future internet. mdpi.com

Lehto M. (2022). "Cyber-attacks against critical infrastructure", *Cyber Security: Critical Infrastructure Protection*, Springer International Publishing.

Leombroni M., Vedolin A., Venter G. and Whelan P. (2021). "Central bank communication and the yield curve", *Journal of Financial Economics*, Vol. 141, No. 3, pp. 860-880.

Liao C. H., Guan X. Q., Cheng J. H. and Yuan S. M. (2022). "Blockchain-based identity management and access control framework for open banking ecosystem", *Future Generation Computer Systems*, Vol. 135, pp. 450-466.

Liu H., Han D. and Li D. (2020). "Fabric-IoT: A blockchain-based access control system in IoT", *IEEE Access*.

Liu X. M. (2021). "A risk-based approach to cybersecurity: A case study of financial messaging networks data breaches", *The Coastal Business Journal*.

Luo A. F., Warford N., Dooley S., Greenstadt R., Mazurek M. L. and McDonald N. (2023). "How library IT staff navigate privacy and security challenges and responsibilities", in: *32nd USENIX Security Symposium*, pp. 5647-5664.

Maiti M., Vuković D., Mukherjee A., Paikarao P. D. and Yadav J. K. (2022). "Advanced data integration in banking, financial, and insurance software in the age of COVID-19", *Software: Practice and Experience*, Vol. 52, No. 4, pp. 887-903.

Makrakis G. M., Kolias C., Kambourakis G., Rieger C. and Benjamin J. (2021). "Industrial and critical infrastructure security: Technical analysis of real-life security incidents", *IEEE Access*, No. 9, pp. 165295-165325.

Mani Z. A. and Goniewicz K. (2023). "Adapting disaster preparedness strategies to changing climate patterns in Saudi Arabia: A rapid review", *Sustainability*.

Marcu M. R. (2021). "The impact of the COVID-19 pandemic on the banking sector", *Management Dynamics in the Knowledge Economy*.

Masuduzzaman M. and Hussain M. I. (2012). "Terms of trade and its implications: Bangladesh perspective", *Working Paper Series: WP 1201*, available online at: http://www.bangladeshbank.org.bd.

Mazumder M. and Sobhan A. (2020). "The spillover effect of the Bangladesh Bank cyber heist on banks' cyber risk disclosures in Bangladesh", *Journal of Operational Risk*.

Mazumder M. M. M. and Hossain D. M. (2023). "Voluntary cybersecurity disclosure in the banking industry of Bangladesh: Does board composition matter?", *Journal of Accounting in Emerging Economies*, Vol. 13, No. 2, pp. 217-239.

McDonald A., Barwulor C., Mazurek M. L., Schaub F. and Redmiles E. M. (2021). "It's stressful having all these phones: Investigating Sex Workers' Safety Goals, Risks, and Practices Online", in: *30th USENIX Security Symposium*, pp. 375-392.

Melito T. (2020). "The adoption of cryptocurrency technology into the US banking infrastructure", available online at: http://www.sc.edu.

Meraj A. I., Samindra S. F., Chhoan T. F., Kashpia A. S. and Ahmed T. (2022). "Preventing national identity forgery in Bangladesh using IGA based security controls", doctoral dissertation, Brac University.

Mhlanga D. (2023). "Block chain for digital financial inclusion towards reduced inequalities", in: *FinTech and Artificial Intelligence for Sustainable Development: The Role of Smart Technologies in Achieving Development Goals*, Cham: Springer Nature Switzerland, pp. 263-290.

Milon M. N. U. and Zafarullah H. (2024). "Uncovering the depths of trade-based money laundering: Evidence from a seaport in Bangladesh", *Journal of Money Laundering Control*.

Moosa A., Ohei K., Raymond E. and Chukwuneme E. P. (2023). "The roles of campus protection services for students' safety: A case of a higher education institution in South Africa", *International Journal of Innovation in Management, Economics and Social Sciences*, Vol. 3, No. 1, pp. 1-11.

Mott G., Nurse J. R. C. and Baker-Beall C. (2023). "Preparing for future cyber crises: Lessons from governance of the coronavirus pandemic", *Policy Design and Practice*.

Mott G., Turner S., Nurse J. R., MacColl J., Sullivan J., Cartwright A. and Cartwright E. (2023). "Between a rock and a hard (ening) place: Cyber insurance in the ransomware era", *Computers & Security*, Vol. 128, p. 103162.

Murinde V., Rizopoulos E. and Zachariadis M. (2022). "The impact of the FinTech revolution on the future of banking: Opportunities and risks", *International Review of Financial Analysis*, Vol. 81, p. 102103.

Nicholls J., Kuppa A. and Le-Khac N. A. (2021). "Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape", *IEEE Access*.

Noor U., Shahid S., Kanwal R. and Rashid Z. (2023). "A machine learning based empirical evaluation of cyber threat actors high level attack patterns over low level attack patterns in attributing attacks", arXiv preprint arXiv:2307.10252.

Ogunode N. J., Edinoh K. and Olatunde-Aiyedun T. G. (2023). "Staff training in schools", *Journal of Innovation in Education and Social Research*, Vol. 1, No. 3, pp. 192-207.

Olivier B. (2021). "The future of the past of a cinematically mediated protest song", *Psychotherapy and Politics International*.

Onwubiko C. and Ouazzane K. (2022). "Challenges towards building an effective cyber security operations centre", arXiv preprint arXiv:2202.03691.

Oruc A., Chowdhury N. and Gkioulos V. (2024). "A modular cyber security training programme for the maritime domain", *International Journal of Information Security*, pp. 1-36.

Pagán A. and Elleithy K. (January 2021). "A multi-layered defense approach to safeguard against ransomware", in: *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0942-0947.

Park H. and Kim J. D. (2020). "Transition towards green banking: Role of financial regulators and financial institutions", *Asian Journal of Sustainability and Social Responsibility*, Vol. 5, No. 1, pp. 1-25.

Park S. (2021). "Evading, hacking & laundering for nukes: North Korea's financial cybercrimes & the missing silver bullet for countering them", *Fordham Int'l LJ*.

Pascarella G., Rossi M., Montella E., Capasso A., De Feo G., Botti G. and Morabito A. Et al. (2021). "Risk analysis in healthcare organizations: Methodological framework and critical variables", *Risk Management and Healthcare Policy*, pp. 2897-2911.

Pearson D. L. (2021). "Chaotic and unexplored: The complex relationship between security professionals, data breaches, and malicious actors", available online at: http://www.proquest.com

Piroska D. and Mérő K. (2021). "Managing the contradictions of development finance on the EU's Eastern periphery: Development banks in Hungary and Poland", *The Reinvention of Development Banking in the European Union*.

Pollmeier S., Bongiovanni I. and Slapničar S. (2023). "Designing a financial quantification model for cyber risk: A case study in a bank", *Safety Science*.

Progoulakis I., Rohmeyer P. and Nikitakos N. (2021). "Cyber physical systems security for maritime assets", *Journal of Marine Science and Engineering*, Vol. 9, No. 12, p. 1384.

Qin M. and Mogos G. (October 2022). "Cyber-attacks on SWIFT systems of financial institutions", in: *Proceedings of the 5th International Conference on Computer Science and Software Engineering*, pp. 596-599.

Rabiul Hasan M. (2024). "Safeguarding of financial organization from cyber-attack using next generation firewall (NGFW), security information & event management (SIEM) and honeypot", available online at: http://www.dbs.ie.

Rahman M. H., Tanchangya T., Rahman J., Aktar M. A. and Majumder S. C. (2024). "Corporate social responsibility and green financing behavior in Bangladesh: Towards sustainable tourism", *Innovation and Green Development*, Vol. 3, No. 3, p. 100133.

Ramirez J. G. C. (2024). "The power of planning: How business plans drive effective management strategies", *Integrated Journal of Science and Technology*.

Ros G. (2020). "The making of a cyber crash: A conceptual model for systemic risk in the financial sector", *ESRB: Occasional Paper Series*.

Ruiz R. S. (2021). "Novel approaches to applied cybersecurity in privacy, encryption, security systems, web credentials, and education", available online at: http://www.londonmet.ac.uk.

Ruvin O., Isaieva N., Sukhomlyn L., Kalachenkova K. and Bilianska N. (2020). "Cybersecurity as an element of financial security in the conditions of globalization", *Journal of Security & Sustainability Issues*, Vol. 10, No. 1.

Safitra M. F., Lubis M. and Fakhrurroja H. (2023). "Counterattacking cyber threats: A framework for the future of cybersecurity", *Sustainability*.

Salvi A., Spagnoletti P. and Noori N. S. (2022). "Cyber-resilience of critical cyber infrastructures: Integrating digital twins in the electric power ecosystem", *Computers & Security*.

Sánchez-Zas C., Villagrá V. A., Vega-Barbas M., Larriva-Novo X., Moreno J. I. and Berrocal J. (2023). "Ontology-based approach to real-time risk management and cyber-situational awareness", *Future Generation Computer Systems*, Vol. 141, pp. 462-472.

Sayduzzaman M., Sazzad S., Rahman M., Rahman T. and Uddin M. K. (2024). "Managing escalating cyber threats: Perspectives and policy insights for Bangladesh", *International Journal of Innovative Science and Research Technology*, Vol. 9, No. 1.

Seth B., Dalal S., Jaglan V., Le D. N., Mohan S. and Srivastava G. (2022). "Integrating encryption techniques for secure data storage in the cloud", *Transactions on Emerging Telecommunications Technologies*, Vol. 33, No. 4, p. e4108.

Settembre-Blundo D., González-Sánchez R., Medina-Salgado S. and García-Muiña F. E. (2021). "Flexibility and resilience in corporate decision making: A new sustainability-based risk management system in uncertain times", *Global Journal of Flexible Systems Management*, Vol. 22, No. Suppl 2, pp. 107-132.

Shakhbazian K. (2021). Cooperation of states in the field of Combating Cyber Crime and approaches to solving the problem of cyber terrorism. Actual Problems of International Relations. iir.edu.ua

Shalabi K., Al-Fayoumi M. and Al-Haija Q. A. (2023, August). "Enhancing financial system resilience against cyber threats via SWIFT customer security framework", in: *2023 International Conference on Information Technology (ICIT)*, pp. 260-265.

Sharma S. and Aparicio E. (2022). "Organizational and team culture as antecedents of protection motivation among IT employees", *Computers & Security*.

Shin B. and Lowry P. B. (2020). "A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished", *Computers & Security*, Vol. 92, doi: https://doi.org/10.1016/j.cose.2020.101761.

Siderius K. (2023). "An unexpected climate activist: Central banks and the politics of the climate-neutral economy", *Journal of European Public Policy*.

Sijan M. A. H., Shahoriar A., Salimullah M., Islam A. S. and Khan R. H. (March 2022). "A review on e-banking security in Bangladesh: An empirical study", in: *Proceedings of the 2nd International Conference on Computing Advancements*, pp. 330-336.

Sikder A. S. and Islam M. R. (2023). "Enhancing cyber-resilience within bangladesh's legal framework: Evaluating preparedness and mitigation strategies against technologically-driven threats — Enhancing cyber-resilience within Bangladesh's legal framework", *International Journal of Imminent Science & Technology*, Vol. 1, No. 1, pp. 40-57.

Soderberg G., Bechara M. M., Bossu W., Che M. N. X., Davidovic S., Kiff M. J. and Yoshinaga A. et al. (2022). "Behind the scenes of central bank digital currency: Emerging trends, insights, and policy lessons", International Monetary Fund (IMF).

Sookhak M., Jabbarpour M. R., Safa N. S. and Yu F. R. (2021). "Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues", *Journal of Network and Computer Applications*, Vol. 178, p. 102950.

Spafford E. H., Metcalf L. and Dykstra J. (2023). *Cybersecurity Myths and Misconceptions: Avoiding the Hazards and Pitfalls that Derail Us*, Addison-Wesley Professional.

Stanikzai A. Q. and Shah M. A. (December 2021). "Evaluation of cyber security threats in banking systems", in: *2021 IEEE Symposium Series on Computational Intelligence (SSCI)*, pp. 1-4.

Stoddart K. (2022). "On Cyberwar: Theorizing cyberwarfare through attacks on critical infrastructure — Reality, potential, and debates", *Cyberwarfare: Threats to Critical Infrastructure*.

Suh J. (2023). "Human rights and corruption in settling the accounts of the past: Transitional justice experiences from the Philippines, South Korea, and Indonesia", *Journal of the Humanities and Social Sciences of Southeast Asia*, Vol. 179, No. 1, pp. 61-89.

Thompson S. A. and Warzel C. (2022). "Twelve million phones, one dataset, zero privacy", *Ethics of Data and Analytics*.

Triplett W. J. (2022). "Addressing human factors in cybersecurity leadership", *Journal of Cybersecurity and Privacy*.

Uchendu B., Nurse J. R. C., Bada M. and Furnell S. (2021). "Developing a cyber security culture: Current practices and future needs", *Computers & Security*.

Uddin M. H., Ali M. H. and Hassan, M. K. (2020). "Cybersecurity hazards and financial system vulnerability: A synthesis of literature", *Risk Management*.

Ul Haque S. (2023). "Analyzing contemporary banking operations: An internship report on evolving challenges and trends", 103.109.52.4.

Ullah F., Qayyum S., Thaheem M. J., Al-Turjman F. and Sepasgozar S. M. (2021). "Risk management in sustainable smart cities governance: A TOE framework", *Technological Forecasting and Social Change*, Vol. 167, p. 120743.

Van Binsbergen J. H., Diamond W. F. and Grotteria M. (2022). "Risk-free interest rates", *Journal of Financial Economics*, Vol. 143, No. 1, pp. 1-29.

Van Greuning H. and Bratanovic S. B. (2020). "Analyzing banking risk: A framework for assessing corporate governance and risk management".

Varga S., Brynielsson J. and Franke U. (2021). "Cyber-threat perception and risk management in the Swedish financial sector", *Computers & Security*.

Wang Q., Ren F. and Li R. (2023). "Exploring the impact of geopolitics on the environmental Kuznets curve research", *Sustainable Development*.

Wanof M. I. (2023). "Digital technology innovation in improving financial access for low-income communities", *Technology and Society Perspectives (TACIT)*, Vol. 1, No. 1, pp. 26-34.

Xu J., Marodon R., Ru X., Ren X. and Wu X. (2021). "What are public development banks and development financing institutions? — Qualification criteria, stylized facts and development trends", *China Economic Quarterly International*, Vol. 1, No. 4, pp. 271-294.

Zafarullah H. and Haque H. (2023). "Policies, instrumentalities, compliance and control: Combatting money laundering in Bangladesh", *Journal of Money Laundering Control*.

Zografopoulos I., Ospina J., Liu X. and Konstantinou C. (2021). "Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies", *IEEE Access*.