The February 2016 Bangladesh Central Bank Cyberattack: Analysing the Incident and Improving Cyber Safety Strategies in a financial institute.

Konara K.M.B.M
IIT Student Id: 20222105
UOW Student ID: w1986540
July 14, 2023,
Word Count: 5230

Abstract—**The cyber attack on the Bangladesh Central Bank in February 2016 highlighted vulnerabilities in financial institutions and the need for improved cybersecurity. Hackers used stolen credentials to move roughly $1 billion over the SWIFT network. While an employee at a non-profit organisation in Sri Lanka discovered a typographical error, halting a substantial transfer, about $81 million reached accounts in the Philippines before the remaining transactions were halted. An international inquiry was launched after the attack, which was blamed on the Lazarus Group. To prevent cyber threats and maintain financial stability, lessons include strengthening security frameworks, adopting authentication methods, and taking proactive actions such as staff training and information exchange.**

Keywords—Cyber attack, bank heist, SWIFT, LazarusGroup, Bangladesh Central Bank attack

I. INTRODUCTION TO HOW THE CYBER ATTACK HAPPENED

The Central Bank of Bangladesh, situated in the city of Dhaka, serves as the custodian of the country's most valuable financial reserves, crucial for the well-being of millions of economically disadvantaged citizens. On the day after the incident(5th of February 2016 morning), a malfunctioning printer located within the highly restricted area of the bank became a cause for concern. This printer was connected to a computer that served as a gateway to the global financial system, responsible for recording and documenting the daily inflow and outflow of millions of dollars. Despite initial attempts by the duty manager, Mr Zubair Bin Huda, to resolve the printer issue, the problem persisted, ultimately leading to his departure from the bank for the day. [1]

The following day(7th of February 2016), upon returning to work, the printer remained non-functional, prompting the authorization to reboot it through an alternate method. Upon completion of the reboot, the bank staff discovered a backlog of printed pages containing numerous million-dollar transactions and urgent requests for clarification. These clarification requests originated from the New York Federal Reserve Bank, the institution responsible for safeguarding Bangladesh's foreign currency reserves, seeking validation of the legitimacy of the transactions. Alarmingly, it was revealed that the entirety of Bangladesh's account, totalling almost 1 billion dollars, had been drained, prompting deep concerns at the New York Federal Reserve Bank.

When the unauthorized transactions executed by the hackers came to light, panic swept through the bank, causing a sense of alarm among the employees. Initially, they suspected that it might have been a mistake on the part of the New York Federal Reserve Bank. Their immediate response was to verify the occurrence of the transactions and halt them promptly. However, confirming the legitimacy of the transactions posed a challenge as it was a Sunday, and unlike many other countries, the weekend holidays in Bangladesh fall on Fridays and Saturdays, while in New York, they are kept on Saturdays and Sundays. Consequently, when the employees in Bangladesh resumed work on Sunday, no one was available in New York to address their concerns. Nevertheless, with concerted efforts, they managed to establish communication with the New York Federal Reserve Bank to ascertain the validity of the transactions.

The response from the New York Federal Reserve Bank provided unequivocal confirmation that the transactions had indeed originated from within the central bank of Bangladesh and were legally executed. However, only five of these instructions successfully transferred funds to the intended destination accounts. The remaining 30 instructions were cancelled due to the detection of several errors that aroused suspicion. Among the five successful transfers, 20 million dollars were transferred to accounts belonging to a Sri Lankan non-governmental organization, while the remaining 81 million dollars were deposited into four fictitious accounts opened in the Philippines. But one notable error was a typographical mistake noticed by an astute employee in Sri Lanka, who identified the misspelling of the word "foundation" as "foundation." This error led to the cancellation of the transaction, preventing a significant loss.

This turn of events revealed the depth of the intrusion and the extent to which the hackers had successfully manipulated the system. Despite the subsequent intervention to stop the unauthorized transactions, a substantial amount of money had already been siphoned off, leaving the Bangladesh Central Bank grappling with significant financial losses and raising concerns about the efficacy of its security measures.

Following their initial attempts to halt the unauthorized transactions, the bank embarked on covert investigations, recognizing the gravity of the situation. To ensure a comprehensive inquiry, the bank promptly engaged cyber security investigators to conduct a thorough examination of the incident. At this stage, the bank faced uncertainty regarding the possibility of reversing or terminating illicit transactions. Subsequent analysis of CCTV footage confirmed that the unauthorized transactions were not carried out through physical access to the SWIFT computer. This revelation raised a perplexing question: how were the funds transferred? The magnitude of the incident dubbed it the world's most significant bank heist, further underscoring the urgency of uncovering the methods employed by the perpetrators.

Summary of the incident

1. Spear Phishing attack launched – early January 2016
2. The attack was launched – 4th of February 2016 evening.
3. In New York, the Federal Reserve Bank was busy processing 35 inquiries about transfers from Bangladesh's central bank. – 5th of February 2016
4. The day of identified that attack was placed – 7th of February 2016

Aftermath

The cyberattack on the Bangladesh Central Bank in February 2016 had significant repercussions, leading to a complex investigation and raising numerous questions about accountability and security measures. The attack involved the laundering of stolen funds through the Philippines, with two Chinese middlemen playing a crucial role in the subsequent investigation. However, their escape to Macao made tracking them nearly impossible. Despite the hackers' attempts to delete traces of malware activities, cybersecurity experts were able to conduct an analysis of the malicious code, which revealed a possible connection to similar attacks on financial institutions worldwide.

The incident shed light on the importance of properly assigning privileges within an organization and implementing strong security practices. The attack likely involved malware being sent via email, which collected usernames and passwords while covering its tracks. Attackers compromised the bank's systems and modified applications, gaining access to the SWIFT terminals responsible for transferring payment orders between organizations and countries. With access to the bank's credentials, the hackers exploited the SWIFT messaging system to send fraudulent messages to the Federal Reserve.

The incident exposed weaknesses in the end points of the SWIFT system within banks, leading to the recognition that financial institutions need to prioritize both physical and cybersecurity measures. The SWIFT organization clarified that there was no indication of a compromise to its core messaging service. In response, a customer security program was launched in 2016 to assist customers in strengthening the security of their SWIFT-related infrastructure. [2]

To mitigate the attack, Bangladesh Bank could have implemented several necessary controls. These included controlling applications to reduce the risk of malware, removing local administrative rights, ensuring unique and secure credentials, enforcing regular password changes, widely implementing multi-factor authentication, segmenting networks, isolating remote access, and monitoring all remote access to highly sensitive systems for threat detection. Taking these steps and prioritizing the security of privileged accounts could have prevented the attackers from carrying out the heist.

While institutions involved in the incident denied responsibility, they took steps to improve their cybersecurity measures. The issue of accountability remained unresolved, with the Bangladesh Senate conducting an inquiry into money laundering. Bangladesh Bank denied involvement from anyone within the bank and any negligence on their part. No individuals were charged by the police in Bangladesh.

The incident prompted inquiries into several possible factors contributing to the event. Questions arose regarding how the malware was activated within the bank's internal system and whether the critical mistake lay with an individual. Security policies and the bank's responsibility for maintaining a safe and secure infrastructure were also under scrutiny. The bank branch manager became a focus of attention, as accounts were opened in RCBC bank in the Philippines under her authority. She opened these accounts based on recommendations from a Manila casino owner for individuals with fake identities.

RCBC bank was fined for failing to comply with regulations. The timing of payments documented in the Senate report raised suspicions, as many were made just minutes apart. The bank manager's lawyer stated that she checked the validity of remittances with the head office and received emails confirming their legitimacy. The lawyer also argued that she lacked the authority to unilaterally prevent fund transfers.[2]

Funds were transferred from RCBC to the Phil Gram remittance company, which laundered the money through casinos. The investigation faced challenges due to the existing Bank Secrecy Act, which provided an unusual level of privacy for bank accounts, making it difficult for investigators to access information. Casinos were frequently used for converting electronic funds into cash, although in this case, there was no evidence suggesting that the casino or its owner were aware of the stolen funds. At the time, casinos were not obligated to report large transactions under money laundering laws.

Recommendations were made to expand the reach of money laundering laws and provide easier access to bank accounts. The Federal Reserve Bank of New York flagged some of the suspicious transactions due to the mention of the name "Jupiter," which coincidentally matched the name of an Iranian tanker. Additionally, the payments differed significantly from Bangladesh Bank's usual transactions, lacking proper formatting and being made to individuals rather than organizations.

While the Federal Reserve systems were not compromised, the event was seen as an opportunity to enhance the security of the global payment system. The Federal Reserve claimed to have been conducting screening and diligence on funds transfers, although some concerns were raised about the timing of inter-bank communication. As no one was held responsible for the financial loss, the focus shifted to tightening security to prevent future attempts. This emphasized the need for a comprehensive cybersecurity strategy that prioritizes risk management, cybersecurity awareness, and preparedness.

II. Technical Details of the Cyber Attack

The cyber-attack against the Bangladesh Central Bank in February 2016 was a sophisticated operation that exploited flaws in the financial institution's security systems. This section gives insight into the technical aspects of the attack, the methods employed by hackers, and the consequences of enhancing cybersecurity strategies in the banking industry.

The attackers first got access to the bank's systems by compromising the credentials of authorised users.[3] It is thought that the breach was caused by the use of malware-infected emails or by exploiting flaws in the bank's network infrastructure. This enabled the hackers to maintain a permanent presence within the bank's network, undetected by existing security procedures.

The attackers, having gained access to the Bangladesh Bank, went on to exploit the SWIFT network, a widely utilized system for international money transfers between banks. Their proficiency in navigating the system suggested prior experience with similar attacks. Exploiting their access to the SWIFT network, they initiated a series of fraudulent transactions using legitimate credentials. Their objective was to transfer around $1 billion from the bank's account held at the Federal Reserve Bank of New York, exploiting the secure communication and transaction authorization provided by SWIFT. This enabled the hackers to attempt significant fund transfers, leveraging their knowledge of the system and the compromised credentials they possessed.

The attackers employed sophisticated techniques to obfuscate their activities and evade detection. Their approach involved manipulating the internal messaging systems of the bank and tampering with transaction records, all with the intention of concealing their illicit operations. By altering the transaction history, they aimed to avoid detection of fraudulent transfers during routine audits, adding an extra layer of camouflage to their activities.

In addition, the hackers utilized advanced evasive strategies to overcome security measures. They developed and deployed custom-made malware specifically crafted to target SWIFT applications. This malicious software allowed them to manipulate and authorize fraudulent transactions without arousing suspicion. Through the malware, the attackers gained the ability to modify account balances, suppress transaction notifications, and ensure that the transactions appeared legitimate within the SWIFT network. By exploiting these capabilities, they effectively bypassed security controls and heightened the challenge of identifying their fraudulent activities.

These advanced tactics employed by the attackers underscore the need for financial institutions to implement multi-layered security measures that go beyond traditional defences. The incident highlights the importance of continuous monitoring, anomaly detection systems, and robust threat intelligence to identify and respond promptly to such sophisticated attacks. By staying vigilant and leveraging advanced cybersecurity tools and practices, organizations can bolster their defences against evolving threats and mitigate the risk of financial fraud within the banking sector.

To execute the attack, the hackers created a complex system that exploited the time disparities inherent in international banking. The transfer of funds from the Bangladesh Bank's New York account to accounts in the Philippines involves three separate time zones. The attackers successfully planned their efforts such that when false payment orders began arriving at the New York Federal Reserve on Thursday afternoon, the Bangladesh Bank was closed for the weekend (which began on Friday). As a result, when the Bangladesh Bank reopened on Sunday, the New York Federal Reserve was on vacation. Taking advantage of the timing, the Bangladesh Bank sought to contact banks in the Philippines, but they, too, were closed for the Chinese New Year, making effective communication much more difficult. The attack occurred at a period when banks were unable to communicate effectively, increasing the attackers' chances of success dramatically. It was too late by the time the banks in their separate countries were able to initiate contact. [4]

Due to a typographical error in one of the five successful fraudulent transaction requests, the attack was only partially successful, prompting further investigation. The mistake prompted Deutsche Bank, one of the intermediate banks involved, to seek clarification from the Bangladesh Central Bank, which eventually led to the discovery of the fraudulent activities**.** [5]

The assault exposed major security flaws in the infrastructure of the Bangladesh Central Bank. It exposed the SWIFT system's vulnerabilities, emphasising the necessity for improved authentication and transaction monitoring methods. Furthermore, the incident highlighted the necessity of staff awareness and training in combating phishing assaults and other forms of social engineering.

The cyber attack on the Bangladesh Central Bank is a sharp reminder of the expanding threat landscape and the potential repercussions of insufficient cybersecurity efforts. It spurred financial institutions throughout the world to rethink their security practises and put in place tighter procedures to protect against such attacks in the future.

To summarise the technical facts, the attack on the Bangladesh Central Bank used a combination of social engineering, malware, and unauthorised financial transfers. The attackers started the attack by sending targeted spear-phishing emails to bank workers.[6] These emails contained malware-laden attachments that, when opened, affected the bank's internal systems. The attackers got access to critical components of the bank's network, including the SWIFT messaging system used for international financial transfers. They used these technologies to send multiple fraudulent payment orders to various global institutions, diverting monies to accounts in the Philippines.

III. Discuss How the Attack Was Detected

The detection of this attack was a variety of fortunate events and the vigilance of the international banking community. Even though the attack resulted in a considerable loss of funds, as a result of the detection and response efforts eventually prevented an even more enormous financial disaster.

The attackers' typographical error during the fraudulent transfer requests was one of the crucial criteria in discovering the scam. The attackers misspelt "foundation" as "fandation" in one of the transaction orders, bringing the notice of Deutsche Bank, one of the intermediary banks engaged in the transfer process. Following the discovery of the inaccuracy, Deutsche Bank contacted the Bangladesh Central Bank to seek an explanation for the transaction, as the error appeared suspicious.

The Deutsche Bank inquiry spurred an examination by the Bangladesh Central Bank, which revealed that fraudulent transactions were taking place. Concurrently, the Federal Reserve Bank of New York became wary of unusual requests. These developments prompted quick action, including attempts to halt further transfers and the involvement of law enforcement agencies. The transactions were highlighted for review, resulting in the freezing of the remaining fraudulent transfers.

The detection efforts were not limited to the financial institutions involved. The Anti-Money Laundering Council in the Philippines, upon noticing the large influx of funds into local banks, also became suspicious and initiated an investigation, contacting the Bangladesh Central Bank to verify the legitimacy of the transactions.[7] Once the attack was confirmed, the Bangladesh Central Bank sought assistance from various international entities, including the U.S. Federal Bureau of Investigation (FBI) and Interpol. These organizations provided technical expertise and collaborated with local law enforcement agencies to gather evidence and track down the perpetrators.

In addition to the typographical error and the attentiveness of banking institutions, following forensic investigation and incident response techniques contributed to the detection of the Bangladesh Central Bank cyber assault. Experts in cybersecurity researched the affected systems, analysing malware, reviewing system logs, and reconstructing the attack timeline. This highlighted the significance of robust monitoring and anomaly detection systems, prompting financial institutions to deploy stronger transaction monitoring methods based on sophisticated analytics and machine learning. The attack served as a wake-up call, forcing global financial institutions to strengthen cybersecurity safeguards, better information sharing, and build stronger communication channels to collectively combat threats. It also emphasised the importance of international law enforcement authorities and financial institutions working together to tackle cybercrime.

IV. TECHNICAL RISKS ASSOCIATED WITH THE CYBERATTACK

The vulnerability of the SWIFT (Society for Worldwide Interbank Financial Telecommunication) messaging system was one of the key technological dangers uncovered by the Bangladesh Bank cyberattack. [7], [8] Malware was used by the attackers to control the SWIFT software installed on the bank's computers, allowing them to initiate fraudulent transactions. This event raised worries about the security of essential financial infrastructure and emphasised the need for more robust protections to secure systems that support global financial transactions.

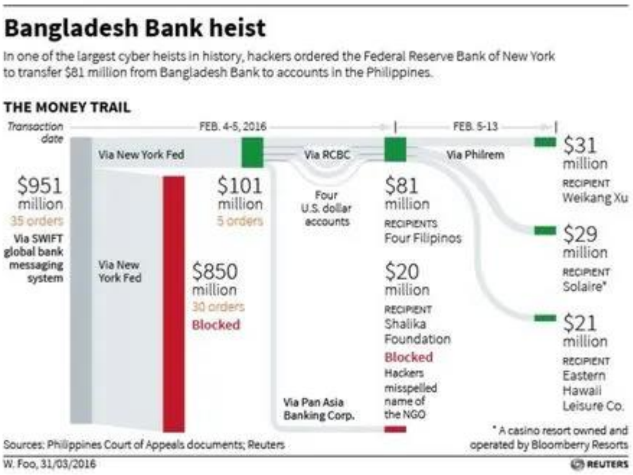

Figure 1 The money trail of the Bangladesh Bank heist. [8]

Another technical concern revealed by this attack was the deployment of sophisticated malware and social engineering tactics.[1], [3] The attackers targeted the bank's employees with cleverly designed spear-phishing emails with malware attachments. Once opened, the malware infected the victim's computer, granting the attackers unauthorised access to the bank's network. This incident highlighted the need to educate employees about the hazards involved with email attachments, as well as the need for comprehensive security mechanisms to identify and prevent such assaults. [6]

The hack on the Bangladesh Central Bank not only highlighted the hazards associated with ineffective or obsolete security procedures, but also underscored the dangers of insider threats. The attackers exploited flaws in the bank's network architecture, utilising them as entry points for their harmful actions. This event served as a clear reminder that organisations must update and patch their systems on a regular basis, implement strong access controls, and undertake frequent security audits to discover and remedy any vulnerabilities. Furthermore, it was later revealed that the attackers had compromised the bank's network months before and were monitoring the employees' activities, highlighting the importance of robust user monitoring, access controls, and employee awareness programmes in mitigating the risk of insider threats. [6]

Furthermore, the attack demonstrated the potential dangers of insider threats.[9] Some of the attackers were determined to have insider knowledge of the bank's operations, including precise facts about the bank's internal procedures and the SWIFT system. This intimate information considerably aided their capacity to successfully orchestrate the attack. To address the dangers posed by insider threats, financial institutions must implement rigorous access controls, regular user monitoring, and constant employee training.

Ultimately, the cyberattack on the Bangladesh Central Bank in February 2016 highlighted various technological concerns connected with cyberattacks on financial institutions. The vulnerabilities in the SWIFT system, network infrastructure, insider threats, sophisticated malware, timely detection and response, and cross-border coordination all pose serious dangers to the global financial system's security. To mitigate these threats and preserve the integrity and trustworthiness of their operations, financial institutions must regularly examine and improve their security procedures.

V. BUSINES RISKS ASSOCIATED WITH THE CYBERATTACK

The cyberattack on the Bangladesh Central Bank in February 2016 had far-reaching business consequences that echoed throughout the financial industry. This attack not only caused enormous financial losses but also disclosed a number of business hazards that organisations should be aware of.

One of the most serious economic concerns linked with the Bangladesh Bank cyberattack was reputational damage. The event garnered extensive media publicity, eroding public faith in the bank's capacity to protect consumer assets. The bank's reputation as a safe financial institution was harmed, raising worries among existing clients and potential investors. Rebuilding confidence in the aftermath of such an assault is a lengthy and difficult process that necessitates major investment in public relations, consumer communication, and transparency.[10]

Another important business risk coming from the cyberattack was financial loss. The attackers attempted to transfer over $1 billion from the bank's account at the Federal Reserve Bank of New York, but only $81 million was successfully transferred due to the identification of several suspicious transactions and inaccuracies in the attackers' requests. Nonetheless, the bank's financial stability suffered as a result of this significant loss, prompting extraordinary efforts to recoup the funds and retain operating viability. To prevent possible financial losses caused by cyberattacks, organisations must have effective risk management procedures.[10]

The hack on the Bangladesh Bank brought to light the organization's potential exposure to legal and regulatory risks following such occurrences. Following the incident, investigations were started to ascertain the reason, evaluate the bank's response, and hold accountable those who were at fault. Failure to deploy sufficient security measures, carry out accurate risk assessments, or properly report breaches may result in fines and penalties from regulatory bodies. Affected parties may also file a lawsuit against the organisation to demand restitution for any harm or financial losses brought on by the assault. To reduce these risks, businesses must implement effective compliance programmes and abide by legal and regulatory regulations.[10]

Significant aftereffects of the incident included operational disruptions and problems with company continuity. The bank's systems failed, forcing a temporary halt to operations. The disruption made it challenging for the bank to conduct routine financial operations, keep an eye on customer accounts, and offer services. The incident showed how important it is to create comprehensive business continuity and disaster recovery plans, including redundant systems, data backups, and alternate processing sites, in order to quickly restore critical services and avoid business impact.[11]

The cyberattack's potential effects on global connections and relationships presented another corporate risk. The attack caused foreign banks and financial institutions to worry about the safety of international transactions. It strained ties between Bangladesh and other global financial players, which can have an effect on trade, investment, and cooperation. In order to reduce this risk, businesses functioning in a globalised economy must place a high value on establishing solid connections and relationships.

The cyberattack on the Bangladesh Central Bank in February 2016 disclosed a number of business dangers related to such attacks, in conclusion. Among these dangers are monetary loss, reputational harm, doubts about the reliability of the banking system, operational difficulties, and legal and regulatory repercussions. To lessen these risks, organisations must take the initiative to develop strong security measures, create efficient incident response plans, and ensure compliance with pertinent regulations. They can protect their financial stability, reputation, and operational continuity by doing this, which will increase their resilience to cyberattacks. Furthermore, industry players must work together to improve cybersecurity overall and preserve public confidence in the financial sector.[6]

VI. DISCUSS OF HOW THE ATTACK CAN BE PREVENTED AND MITIGATED

The cyberattack on the Bangladesh Central Bank in February 2016 brought attention to the necessity for strong cybersecurity measures to stop and lessen such attacks. In here, we'll examine the attack and discuss how to make financial institutions' online security better. Financial institutions must prioritise network security, user awareness and training, incident response planning, vendor management, and regulatory compliance in order to prevent and mitigate cyberattacks. By implementing robust security measures and adhering to industry regulations, organizations can enhance their resilience to cyber threats, safeguard their financial stability, and maintain trust in the banking system.

Financial institutions should put network security first. In order to do this, multi-layered defences including firewalls, intrusion detection and prevention systems, and secure web gateways must be put in place. To find and fix any holes in the network infrastructure, routine penetration tests and vulnerability assessments should be carried out. To prevent unauthorised access, rigorous access controls should be installed, such as two-factor authentication and privileged access management. Segmenting the network can prevent attackers from moving laterally through it.[12]

The second important factor is user education and awareness. It is important to inform staff members of the dangers posed by phishing, social engineering, and malware attachments. Regular training sessions can teach staff how to spot malicious emails, browse safely, and report potential security concerns right away. To evaluate the success of the training programme and pinpoint areas for development, simulated phishing exercises can be used. In order to stop successful assaults, employers must foster a culture of cybersecurity awareness and alertness among their workforce. [13]

Third, there must be detailed incident response strategies in place for financial institutions. In these plans, the procedures to be followed in the case of a cyberattack should be specified, along with communication protocols, roles, and duties, and coordination with law enforcement organisations. Regular tabletop exercises and mock emergency response drills can help find weaknesses in the plan and strengthen response capabilities. The ability to promptly identify, contain, and mitigate cyber risks requires well-trained incident response teams with access to the required technologies and resources.

A crucial aspect of cybersecurity is vendor management, which is the fourth point. Third-party vendors are frequently used by financial institutions to provide a range of services, which might lead to further weaknesses. It's crucial to evaluate the security procedures followed by vendors, to exercise diligence, and to create strong contractual agreements that expressly state what kind of security is expected of them. To ensure adherence to security standards, routine vendor audits and evaluations should be carried out. Supply chain attack risk can also be reduced by monitoring and managing unauthorised access to the network and sensitive information.

Finally, financial institutions must adhere to all applicable laws and norms. Good cybersecurity practises are facilitated by adherence to standards that are specific to the industry, such as the General Data Protection Regulation (GDPR), and Payment Card Industry Data Security Standard (PCI DSS). To check compliance and address any concerns with non-compliance, regular audits and assessments should be carried out. Insights on new dangers and best practises can be gained via interacting with regulatory bodies, business associations, and information-sharing platforms.

The Bangladesh Bank cyberattack emphasises the need for ongoing monitoring and threat intelligence in addition to these preventive and mitigation measures. Investments in security analytics, advanced threat detection systems, and security information and event management (SIEM) solutions are recommended for financial institutions. The detection and response to threats can be improved by the real-time monitoring and analysis of network traffic, system logs, and user activity. Working together with colleagues in the same industry, sharing threat information, and using cybersecurity information-sharing platforms can give participants insightful knowledge about how threats are changing.[12]

Additionally, financial institutions should think about incorporating cutting-edge technology like machine learning (ML) and artificial intelligence (AI) into their cybersecurity plans. Algorithms powered by AI and ML can analyse enormous volumes of data, spot anomalies, and spot potential security incidents. These innovations can speed up threat identification and response while enhancing human capabilities.

Ensure that your software and systems remain consistently updated with the latest versions and patches. Cyber attacks frequently exploit vulnerabilities resulting from outdated systems or software, thereby gaining unauthorized access to networks. Taking proactive measures to address this risk is essential. Investing in a comprehensive patch management system can effectively manage software and system updates, ensuring the ongoing resilience and up-to-dateness of your system. By implementing such a system, organizations can significantly reduce the likelihood of successful cyber attacks, as timely patches and updates help to address known vulnerabilities, strengthening the overall security posture. This proactive approach to maintaining system integrity is a crucial component of a robust cybersecurity strategy. [13]

Risk mitigation refers to the application of security policies and practices to reduce the impact of a cybersecurity attack. It involves three components: prevention, detection, and remedy. As hackers become more sophisticated, organizations must adapt their vulnerability mitigation measures to stay ahead. Cybercrime has surged by approximately 300% in recent years, with increased threat volume and complexity. Hackers employ evasive tactics and target high-value assets, including IoT devices. Risks such as credential harvesting and ransomware are on the rise, and some hackers even use cloud infrastructure to blend in with legitimate businesses.[12] So, it is crucial to emphasise the necessity of financial institutions having a thorough framework for cybersecurity governance, such as ISO 270001:2022 (Information Security Management System - ISMS). This includes having clear policies and processes, doing frequent risk assessments, and having executive-level management oversee cybersecurity projects. Cybersecurity should be taken seriously at the board level and incorporated into the organization's overall risk management plan.

In conclusion, the hack on the Bangladesh Bank serves as a strong warning regarding the significance of effective cybersecurity measures in financial institutions. Institutions should prioritise network security, user awareness and training, incident response planning, vendor management, and regulatory compliance in order to prevent and mitigate such incidents. The adoption of innovative technology, constant surveillance, and threat intelligence can all help cybersecurity measures work better. Financial institutions may bolster their cybersecurity defences and protect their operations, client data, and reputation in an increasingly digital environment by putting these strategies into practise and encouraging a cybersecurity culture.

REFERENCES

[1] "BBC World Service - The Lazarus Heist," *BBC*. https://www.bbc.co.uk/programmes/w13xtvg9 (accessed Jul. 13, 2023).

[2] "(25) Case Study on Bangladesh Banking Heist | LinkedIn." https://www.linkedin.com/pulse/case-study-bangladesh-banking-heist-digialert/ (accessed Jul. 13, 2023).

[3] "RCBC manager, others face anti-money laundering complaint," *RAPPLER*, Mar. 15, 2016. https://www.rappler.com/business/125901-amlc-money-laundering-complaint-rcbc-manager-deguito/ (accessed Jul. 13, 2023).

[4] "Malware: Bangladesh Bank Heist - Cybersecurity | Digital Forensics | Crypto Investigations." https://ermprotect.com/blog/malware-bangladesh-bank-heist/ (accessed Jul. 03, 2023).

[5] "Nation State Hackers Case Study: Bangladesh Bank Heist – cyber.uk." https://cyber.uk/areas-of-cyber-security/cyber-security-threat-groups-2/nation-state-hackers-case-study-bangladesh-bank-heist/ (accessed Jul. 03, 2023).

[6] "How a spelling mistake stopped hackers stealing $1bn in a bank heist," *The Independent*, Mar. 11, 2016. https://www.independent.co.uk/news/world/asia/spelling-

mistake-stops-hackers-stealing-1-billion-in-bangladesh-bank-heist-a6924971.html (accessed Jul. 13, 2023).

[7] “The Bangladesh Bank Heist: Lessons In Cyber Vulnerability,” *The One Brief*, Jun. 01, 2017. https://theonebrief.com/the-bangladesh-bank-heist-lessons-in-cyber-vulnerability/ (accessed Jul. 03, 2023).

[8] “Special Report: Cyber thieves exploit banks’ faith in SWIFT transfer network,” *Reuters*, May 20, 2016. Accessed: Jul. 13, 2023. [Online]. Available: https://www.reuters.com/article/us-cyber-heist-swift-specialreport-idUSKCN0YB0DD

[9] “Exclusive: Bangladesh probes 2013 hack for links to central bank heist,” *Yahoo News*, May 25, 2016. https://www.yahoo.com/tech/exclusive-bangladesh-probes-2013-hack-links-central-bank-201427456--sector.html (accessed Jul. 13, 2023).

[10] “4 big risks cyber attacks pose for financial institutions.” https://fieldeffect.com/blog/financial-institutions-cyber-risks/ (accessed Jul. 13, 2023).

[11] M. Khorev, “5 cybercrime effects on businesses,” *Red Points*, Sep. 20, 2022. https://www.redpoints.com/blog/effects-of-cybercrime-on-business/ (accessed Jul. 13, 2023).

[12] “Cyber Threats How financial institutions can mitigate risk - Planet Compliance,” *https://www.planetcompliance.com/*. https://www.planetcompliance.com/cyber-threats-how-financial-institutions-can-mitigate-risk/ (accessed Jul. 13, 2023).

[13] “10 Ways to Prevent Cyber Attacks,” *Leaf*, Feb. 11, 2020. https://leaf-it.com/10-ways-prevent-cyber-attacks/ (accessed Jul. 13, 2023).