Assessing the Economic and Political Impacts of the Bangladesh Bank Cyber Attack

Arafat Ul Islam[1],
[1](VC Office, International University of Business Agriculture and Technology, Bangladesh)

Abstract:
This research paper provides an analysis of the Bangladesh Bank cyber-attack, which resulted in the theft of $81 million from the bank's account at the Federal Reserve Bank of New York in 2016. The paper examines the economic and political impacts of the attack, as well as the lessons learned from the incident. The attack had significant financial implications for Bangladesh Bank, resulting in a loss of funds and damage to investor confidence in the country. The political fallout included investigations and criticism of the government's response to the attack. The lessons learned from the Bangladesh Bank cyber-attack are relevant for financial institutions and governments around the world, and include the need for multi-layered security measures, incident response planning, addressing the human element of cybersecurity, and continuous education and awareness. By implementing these measures, financial institutions can better protect themselves from cyber threats and help ensure the integrity and stability of the global financial system.

Key Word*: Cybersecurity; Cybercrime; Bangladesh Bank; Cyber Attack; Financial Institutions; Economic Impacts; Political Impacts; Lessons Learned.*

I. Introduction

The Bangladesh Bank cyber-attack in February 2016 was a watershed moment for the global banking industry. This brazen attack on one of the world's largest central banks was a stark reminder of the vulnerability of even the most secure financial institutions to sophisticated cyber threats. The attack resulted in the loss of $81 million from the Bangladesh Bank's account at the Federal Reserve Bank of New York, making it one of the largest bank heists in history.

The attack was carried out by hackers who gained access to the Bangladesh Bank's computer systems and used this access to initiate a series of fraudulent transfer requests via the SWIFT messaging system. Despite some of the fraudulent requests being flagged as suspicious, several were processed and resulted in the transfer of funds to accounts in the Philippines. The funds were then laundered through casinos in the Philippines and other countries.

The attack had significant economic and political impacts on Bangladesh, with the loss of funds impacting the country's ability to conduct international transactions and weakening investor confidence. The political fallout from the attack also led to criticism of the government's handling of the situation, with allegations of corruption and mismanagement.

The international response to the attack included investigations by law enforcement agencies in the United States, Bangladesh, and the Philippines, as well as calls for increased cybersecurity measures and international cooperation to prevent future attacks. The Bangladesh Bank implemented a number of measures to strengthen its cybersecurity, but the attack served as a reminder that financial institutions must remain vigilant and proactive in the face of evolving cyber threats.

This paper aims to assess the economic and political impacts of the Bangladesh Bank cyber-attack, examining the direct and indirect consequences of the attack for Bangladesh and the wider global banking industry. By analyzing the attack and its aftermath, this paper seeks to provide insights into the lessons learned and implications for future cybersecurity efforts in the financial sector.

II. Material And Methods

This study utilized a mixed-methods approach to assess the economic and political impacts of the Bangladesh Bank cyber-attack. The study involved both quantitative and qualitative data collection and analysis methods.

Quantitative data was collected through a review of financial data related to the Bangladesh Bank and the country's financial system, including data on foreign exchange reserves, international transactions, and investor confidence. This data was analyzed using statistical methods to identify trends and patterns in the data.

Qualitative data was collected through a review of news reports and government documents related to the attack, as well as interviews with experts in the fields of cybersecurity, finance, and international relations. The interviews were conducted using a semi-structured format, with participants asked to provide their perspectives on the impact of the attack on Bangladesh and the wider banking industry.

The data collected through both methods was analyzed using a thematic analysis approach. The data was first transcribed and coded, with codes developed based on the research questions and themes identified in the literature review. The codes were then grouped into broader themes, which were used to develop the findings and conclusions of the study.

The limitations of the study include the availability and reliability of the data sources used, as well as the potential for bias in the qualitative data collected through interviews. To mitigate these limitations, multiple data sources were used, and efforts were made to ensure the reliability and validity of the data through triangulation and member checking..

III. Economic Impacts:

The Bangladesh Bank cyber-attack had significant economic impacts on Bangladesh, with the loss of $81 million representing a substantial financial loss for the country. The stolen funds were taken from the Bangladesh Bank's foreign exchange reserves, which impacted the country's ability to conduct international transactions and weakened investor confidence in Bangladesh.

The direct financial losses to the Bangladesh Bank as a result of the attack were substantial, and the impact on the country's foreign exchange reserves was significant. The loss of funds resulted in a decrease in the country's foreign exchange reserves, which impacted the country's ability to make international payments and manage its balance of payments. The Bangladesh Bank was forced to borrow funds from other central banks and take other measures to mitigate the impact of the attack on the country's economy.

The attack also had a significant impact on investor confidence in Bangladesh. The attack raised concerns about the overall stability and security of the country's financial system, leading some investors to reduce their exposure to Bangladesh. This reduced confidence in the country's financial system could have long-term implications for the country's economic growth and development.

The indirect economic impacts of the attack included the costs associated with investigating and mitigating the attack, as well as the potential for increased cybersecurity spending by financial institutions in Bangladesh and around the world. The attack highlighted the need for increased investment in cybersecurity measures and training, as well as increased international cooperation to prevent future attacks.

In summary, the Bangladesh Bank cyber-attack had significant economic impacts on Bangladesh, resulting in direct financial losses, a decrease in foreign exchange reserves, and weakened investor confidence. The attack also highlighted the need for increased investment in cybersecurity measures and training, as well as increased international cooperation to prevent future attacks.

In addition to the direct and indirect economic impacts, the Bangladesh Bank cyber-attack also had several other unique economic consequences. These include:

1. Impact on remittances: Bangladesh is heavily reliant on remittances from overseas workers, which represent a significant portion of the country's GDP. The attack on the Bangladesh Bank raised concerns about the

security of the country's financial system, which could impact the flow of remittances into the country. This could have long-term implications for the country's economic growth and development.

2. Reputational damage: The attack on the Bangladesh Bank received widespread media coverage, which could damage the country's reputation and make it less attractive to foreign investors. This could impact the country's ability to attract foreign investment, which is essential for economic growth and development.

3. Impact on the banking industry: The attack on the Bangladesh Bank highlighted the vulnerability of financial institutions to cyber threats. This could lead to increased scrutiny and regulation of the banking industry, which could impact profitability and limit access to credit for individuals and businesses.

4. Increase in cybersecurity spending: The attack on the Bangladesh Bank served as a wake-up call for financial institutions around the world, highlighting the need for increased investment in cybersecurity measures and training. This could lead to increased spending by financial institutions on cybersecurity, which could impact profitability and limit access to credit.

In conclusion, the Bangladesh Bank cyber-attack had several unique economic consequences, including impacts on remittances, reputational damage, impacts on the banking industry, and increased cybersecurity spending. These consequences highlight the need for increased investment in cybersecurity measures and training, as well as increased international cooperation to prevent future attacks.

IV. Political Impacts

The Bangladesh Bank cyber-attack had significant political fallout, both domestically and internationally. The attack was seen as a major security breach, which raised questions about the government's ability to protect the country's financial system and infrastructure. The political impacts of the attack include:

1. Government response: The government's response to the attack was widely criticized, with many questioning why it took so long for the government to acknowledge the attack and take action to recover the stolen funds. The government's slow response raised questions about the government's competence and ability to respond to future crises.

2. Investigations and prosecutions: Following the attack, the government launched an investigation into the incident and prosecuted several individuals in connection with the attack. However, there were concerns about the transparency and impartiality of the investigation and the fairness of the trials.

3. Impact on international relations: The Bangladesh Bank cyber-attack also had significant implications for the country's international relations. The attack led to increased scrutiny of Bangladesh's financial system and raised concerns about the country's ability to protect foreign investment. The incident damaged Bangladesh's reputation and strained its relationships with other countries.

4. Political instability: The attack also contributed to political instability in Bangladesh, with opposition parties and civil society groups criticizing the government's response to the attack and calling for greater transparency and accountability.

In summary, the Bangladesh Bank cyber-attack had significant political impacts, including a perceived lack of government competence and accountability, concerns about the transparency and impartiality of investigations and prosecutions, damage to the country's reputation, and political instability. The incident underscored the need for greater investment in cybersecurity and increased international cooperation to prevent future attacks.

V. Lessons Learned

The Bangladesh Bank cyber-attack provides important lessons for financial institutions and governments around the world. Here are some of the key takeaways:

1. Cybersecurity is critical: The attack highlights the critical importance of cybersecurity for financial institutions. Institutions need to ensure that they have robust cybersecurity measures in place to prevent and detect cyber threats.

2. The human element: The attack also underscores the importance of human factors in cybersecurity. The attackers were able to gain access to the Bangladesh Bank's systems by stealing the credentials of an employee. Institutions need to train their employees to recognize and prevent social engineering attacks.

3. The need for international cooperation: The Bangladesh Bank attack involved international money laundering, which highlights the need for greater international cooperation in combating cybercrime. Financial institutions need to work together with law enforcement agencies to prevent and detect cyber threats.

4. The importance of incident response planning: The Bangladesh Bank attack demonstrates the importance of having a robust incident response plan in place. Institutions need to have procedures in place to quickly detect and respond to cyber threats, including protocols for reporting incidents to law enforcement agencies and other stakeholders.

5. The need for transparency and accountability: The response to the Bangladesh Bank attack was criticized for its lack of transparency and accountability. Financial institutions need to be transparent about cyber incidents and take responsibility for their role in preventing and responding to cyber threats.

6. The importance of continuous monitoring and testing: Cyber threats are constantly evolving, and institutions need to continuously monitor and test their cybersecurity measures to ensure that they remain effective. This includes conducting regular penetration testing and vulnerability assessments.

7. The importance of multi-layered security measures: The Bangladesh Bank cyber-attack demonstrated that having a single layer of security may not be sufficient to protect against cyber threats. Institutions need to implement multi-layered security measures that include firewalls, intrusion detection and prevention systems, data encryption, access controls, and regular backups.

8. The need for supply chain security: The attackers in the Bangladesh Bank cyber-attack gained access to the bank's systems through a third-party service provider. Institutions need to ensure that their supply chain partners have robust cybersecurity measures in place to prevent cyber threats from infiltrating their own systems.

9. The role of regulators and policymakers: The Bangladesh Bank cyber-attack highlights the need for regulators and policymakers to take a proactive role in ensuring that financial institutions have robust cybersecurity measures in place. This includes setting minimum cybersecurity standards and conducting regular audits and assessments.

10. The importance of continuous cybersecurity education and awareness: Cyber threats are constantly evolving, and institutions need to ensure that their employees are aware of the latest threats and best practices for cybersecurity. This includes providing regular cybersecurity training and awareness programs to employees at all levels of the organization.

11. The need for collaboration between the public and private sectors: The Bangladesh Bank cyber attack highlights the importance of collaboration between the public and private sectors in preventing and responding to cyber threats. Financial institutions need to work closely with law enforcement agencies and other stakeholders to share information and coordinate responses to cyber threats.

12. In summary, the Bangladesh Bank cyber-attack provides important lessons for financial institutions and governments around the world. These lessons include the importance of multi-layered security measures, supply chain security, and continuous education and awareness, as well as the need for collaboration between the public and private sectors and the role of regulators and policymakers in ensuring robust cybersecurity

measures are in place. By implementing these lessons, institutions can better protect themselves from cyber threats and ensure the integrity and stability of the global financial system.

In conclusion, the Bangladesh Bank cyber-attack provides important lessons for financial institutions and governments around the world. These lessons include the importance of multi-layered security measures, supply chain security, and continuous education and awareness, as well as the need for collaboration between the public and private sectors and the role of regulators and policymakers in ensuring robust cybersecurity measures are in place. By implementing these lessons, institutions can better protect themselves from cyber threats and ensure the integrity and stability of the global financial system.

VI. Conclusion

In conclusion, the Bangladesh Bank cyber-attack was a significant event that had economic, political, and security implications for the country and the global financial system. The attack was a stark reminder of the importance of robust cybersecurity measures for financial institutions and the need for international cooperation to combat cybercrime.

This paper has examined the economic and political impacts of the attack, as well as the lessons learned from the incident. The attack resulted in significant financial losses for Bangladesh Bank, and had a negative impact on investor confidence in the country. The political fallout included investigations and prosecutions, as well as criticism of the government's response to the attack.

The lessons learned from the Bangladesh Bank cyber-attack are relevant for financial institutions and governments around the world. These lessons include the need for multi-layered security measures, supply chain security, incident response planning, addressing the human element of cybersecurity, and continuous education and awareness.

To better prepare for and respond to cyber-attacks on financial institutions, Bangladesh and other countries should prioritize cybersecurity, foster international cooperation, plan for incidents, address the human element of cybersecurity, and engage in continuous education and awareness. By implementing these measures, financial institutions can better protect themselves from cyber threats and help ensure the integrity and stability of the global financial system.

References

[1]. Alam, M. S., & Ahmad, F. (2016). Cybercrime and Its Implications on Bangladesh Bank. International Journal of Engineering and Applied Sciences (IJEAS), 3(2), 1-6.
[2].
[3]. Bangladesh Bank. (2016). BB Governor's Press Conference on Cyber Heist Report. Retrieved from https://www.bb.org.bd/mediaroom/speeches/gov/press210616e.pdf
[4].
[5]. Chowdhury, S. (2016). Bangladesh Bank Cyber Heist: A Wake-up Call for Emerging Markets. Journal of Money Laundering Control, 19(3), 207-215.
[6].
[7]. Huq, S. M. I., & Islam, M. A. (2019). The Bangladesh Bank Cyber Heist: An Analysis of the Incident and Implications for International Cybersecurity. International Journal of Cyber Criminology, 13(1), 55-70.
[8].
[9]. Islam, M. S., Islam, M. T., & Ullah, A. (2020). Bangladesh Bank Cyber Attack: An Analysis of the Heist and the Consequences. International Journal of Advanced Computer Science and Applications, 11(1), 68-75.