Bangladesh Bank Heist 2016

Submitted to :

S M Taiabul Haque

Submitted by :

Name : Nowshin Sumaiya
Id : 21301276
Section : 01
Course : CSE490

In this golden era of modern technologies making our life easier, can it ever be the reason for the loss of millions of dollars for technologies? Think of a quiet room, a computer screen, and a single click that changes everything. No chase scenes, no dramatic environment just hackers working, turning digital loopholes into goldmines. Hackers are sitting miles apart from us, yet working together to find loopholes using modern technologies. They do not need any guns, swords, boomerangs, bombs etc. They only need their PCs, coding skills, and clever ideas. Computer hackers do not need to know each other's real names, or even live on the same continent, to steal millions in mere hours (Mueller, n.d.). Isn't this quite shocking to believe that thieves are not near us, they are behind the computer screen? Welcome to the period of the online bank heist, where millions can vanish with a single click. Compared to other businesses with an online presence, financial institutions are considered to be 300 times more at risk for attacks (Eichler, n.d.). Additionally, from financial losses to reputational damage, to penalties, to insurability issues, to legal liabilities and beyond, there are many bad things that can come from cyber incidents. Cyberattacks also hamper the trust of customers, making them think their money isn't safe. There is more at risk than ever in today's interconnected world and the reason is cyber attack.

The phrase "A Million Dollar Heist" simply has the power to shiver sensitive individuals from a developing nation. But for many Bangladeshi citizens, this is their nightmare in real life. In February 2016, hackers grabbed $101 million from Bangladesh Bank's account at the Federal Reserve Bank of New York, according to a Dhaka Tribune report (Bangladesh Bank Heist: Probe Report Submission Deferred for 78th Time, 2024). The Society for Worldwide Interbank Financial Telecommunication (SWIFT) network, which enables banking organizations and financial institutions to transfer funds through a secure network, was used by the Bangladesh Bank and other banks to transfer their funds to numerous banks across the globe during the attack (Kabir,2023).

Furthermore, despite the fact that the incident happened in 2016, the hackers had long since planned and prepared. The whole incident began with a fraudulent email. Hackers executed this plan on the weekend of Bangladesh's friday, saturday. So that the central bank would be closed and no one could destroy their plan. Since Bangladesh Bank employees were unaware of the fraudulent transactions until Sunday morning, the crime was discovered too late. A large portion of the cash had already been transferred by that time. Using the time difference between Bangladesh, New York, and the Philippines as well as the weekend, the hacker team created the perfect plan for the entire heist, which took five days to carry out. Again, when the Bangladesh Bank authority took the initiative to bring back the looted money, it was not an easy task for them at all.

Let's now explore the fascinating tale of the Bangladesh Bank Heist in more detail. The entire story began with a fraudulent email. Russell Ahlam, an unknown individual, submitted a job application, a cover letter and resume to Bangladesh Bank's management by email in January 2015 (Business Inspection BD,2021). But it wasn't just any job application; subsequently, a malicious program was attached to the file. It was discovered during investigations that a bank employee had unintentionally accessed a malicious application via a defective email, giving hackers access to the bank's network and sensitive data.

Additionally, the printer of Bangladesh's central bank, which was linked to SWIFT software, broke down on February 4, 2016. The problem was identified by the director, who resolved it that same day. They were shocked to discover that transactions were printing out more often than they were expecting after activating the printer. Thirty-five suspicious payment orders for huge amounts of money moved from the bank's private account to numerous accounts across several nations were found by the director and employees. The military-grade security features of the SWIFT system were not functioning as expected. Three messages containing payment orders from the Federal Reserve Bank of New York were recovered when the director and employees gathered around the specialized Swift computer to restart the software.

After gaining access to the bank's system through malware that was deployed in January 2016, the hackers were able to issue payments via the SWIFT network. Since Bangladesh bank’s had an account with a lot of money for international agreements, the hackers decided to target the Federal Reserve Bank of New York. Since the transfer requests were sent by valid SWIFT instructions, the Federal Bank in New York had no justification for stopping them.

After everyone believed that everything was finished, the bank in New York unexpectedly marked 30 of these payments for manual review since the shipping company was on a US-Iranian blacklist. This prevented 871 million USD in transfers, while 101 million USD in transactions could not be stopped (Bento & Harris, 2018). The initial transfer was sent to an NGO in Sri Lanka via a German bank in Frankfurt. Additionally, the $20 million USD of the transfer to Pan Asia Bank in Sri Lanka raised suspicions. It was discovered that the NGO's name was nothing but a scam after the German account pointed out a spelling error (Business Inspection BD,2021). As a result of the hackers' mistakes in spelling, the $20 million transfer to Sri Lanka was unsuccessful. Following that, hackers planned the final four transfers, which were going to a Philippine bank. Due to the Philippines' New Year's celebration, the money was very quickly laundered into cash and casinos, making it untraceable, despite the New York Bank's request. $81 million was moved from Bangladesh Bank's account to the Kim Wanges 4 accounts

by the Federal Reserve Bank. They later divided the entire amount to Phill Ram, a remittance company.

The Bangladesh Bank authorities found it extremely difficult to retrieve the stolen money from the Philippines when they took the initiative to attempt it. The cash flow could not be traced because of the Philippine Bank Secrecy Act. Even the bank statements for Phill Ram and Kim Wang were not given to them. The Philippines, Switzerland, and Lebanon uphold the strictest banking secrecy in the world, according to Senate Inquiries.This would have prevented Bangladesh from losing $81 million if they had given the investigators proper evidence(Business Inspection BD,2021).

An internal control failure that affected not only Bangladesh Bank, but also the New York Fed and SWIFT messaging system, lies at the core of this issue. A global investigation is required to completely comprehend the entire network responsible for this extraordinary cybercrime. From the start, the Bangladeshi government and central bank authority remained silent while the Philippine Senate led the investigation. The possible recovery of the stolen funds is being further harmed by this ongoing secrecy. There is also risk to the developing international payment settlement platform. The government ought to make sure the inquiry is properly conducted. Now, if we consider the idea of risk, Risk = Likelihood x Impact.

Vulnerabilities and threats determine likelihood, and a threat is an actor with the potential and motivation to do bad. Some speculate that the hackers involved in this crime may have had ties to North Korea (Bento & Harris, 2018). The Los Angeles FBI team discovered that the hidden computer code was in Korean and that the IP address matched those of North Korea, according to the BBC podcast. They are therefore motivated and have the ability to carry out such an attack. In order to obtain the bank's SWIFT credentials, the hackers used malware known as "SWIFT Client" to infiltrate the computer systems of the bank. Over a period of a year, the attackers gained access to a bank's network by means of an employee mistake. They set up trusted Windows software and planted malware to keep an eye on bank workers' activity. In addition, hackers installed monitoring software and acquired local admin credentials in order to analyze financial messages and locate services. They then submitted a number of transfer requests to the Federal Reserve Bank of New York, disguising the transfers with fictitious nonprofits and charities to make it challenging for law enforcement to track down the money. The hackers gained access to the bank's systems weeks before the attack, which included insider assistance, social engineering, and malware. This kind of attack could occur due to Bangladesh Bank's system vulnerabilities. This attack will have a big effect. Nearly $81 million was lost, despite some money being recovered, which had an effect on Bangladesh's economy and banking industry.

So many twists and turns in this story leave us with invaluable Lessons learned from the Bangladesh Bank Heist!

- Improve the security protocols.
- Never click on links or open attachments from unreliable sources. A straightforward email can serve as an entry point for attackers.
- Frequent credential changes could stop hackers from keeping network access.
- To stop such attacks, it is best to employ strong malware detection software.
- Restrict access to significant systems, such as SWIFT, and keep an eye out for suspicious activity on privileged accounts.
- In these types of situations, security experts can guarantee unique and non-repeated credentials by removing admin permissions from users.
- Update firmware, software, and security patches frequently to guard against vulnerabilities.
- Create a well-defined communication strategy for dealing with the public and other stakeholders both during and after a breach.
- It is necessary to provide employees with thorough security awareness training in order to educate them of the dangers posed by phishing attacks.
- To prevent insider involvement, it is suggested to establish internal security measures and conduct regular audits and monitoring of user activity and access privileges.

The cyberattack on Bangladesh Bank is an alarming instance of the delicate balance between technical defenses and human weaknesses. Not only was the Bangladesh Bank Heist a criminal act, but it also served as a warning to the whole banking industry. It revealed weaknesses, exposed international banking systems to the test, and demonstrated how one email might ruin millions of dollars. The Bangladesh Bank story reflects a strong desire for alertness, flexibility, and unshakable resilience in this work of security. To wrap up, in the current digital era, where our money is stored by numbers in a computer, strong digital safeguards are now more important for its security than physical locks. Although banks are putting a lot of effort into staying ahead of cyber threats, the battle for security is far from over. The bright side is that each online bank

hack teaches valuable insights that have been used to create more robust defenses and dependable systems. Even if security is never flawless, we can remain hopeful because of the continuous cooperation between cybersecurity professionals and tech innovators.

References

Business Inspection BD (2021, August 09).The Bangladesh Bank Cyber Heist: One of The Largest Bank Robbery in the History. *Business Inspection.* https://businessinspection.com.bd/the-bangladesh-bank-cyber-heist/

Sayegh, E. (2023, June 06). Potential For Devastation: The Impact Of A Cyberattack On The Banking System. *Forbes.* https://www.forbes.com/sites/emilsayegh/2023/06/06/potential-for-devastation-the-impact-of-a-cyberattack-on-the-banking-system/

Dhaka Tribune. (2024, May 06). Bangladesh Bank heist: Probe report submission delayed again. *Dhaka Tribune* https://www.dhakatribune.com/bangladesh/court/345756/bangladesh-bank-heist-probe-report-submission

ISACA. (2023, December 06). Lessons learned from the Bangladesh Bank heist. *ISACA Journal, Volume 6.* https://www.isaca.org/resources/isaca-journal/issues/2023/volume-6/lessons-learned-from-the-bangladesh-bank-heist

Klaassen L(2023, November 24) Unravelling the Bangladesh Bank Cyber Heist: Lessons Learned and Cybersecurity Recommendations. *It Happens*. https://www.ithappens.nu/unravelling-the-bangladesh-bank-cyber-heist-lessons-learned-and-cybersecurity-recommendations/

Kuepper J, Eichler R (2024,May 18). Cyberattacks and the Risk of Bank Failures. *Investopedia.* https://www.investopedia.com/articles/personal-finance/012117/cyber-attacks-and-bank-failures-risks-you-should-know.asp