Module Code & Module Title

CC4004NI Cyber Security Fundamentals

Assessment Weightage & Type

50% Individual Coursework

Year

AY 2023 - 2024

Student Name: ROHAN PRASAD ADHIKARI

London Met ID: 23047505

College ID: NP01NT4A230177

Assignment Due Date: 5th May 2024

Assignment Submission Date: 5th May 2024

Word Count: 3026

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Table of Contents

Table Of Tables:

Table Of Figures:

1. Introduction

1.1. Introduction

The golden era of information technology is upon us. We store all of our information online these days. Knowledge, it was once said, is power. However, given the state of the world today, it is safe to say that knowledge is power. We have made everything in our digital age dependent on the internet, including e-commerce and e-society. We cannot function without internet for even just one second. Because of the amount of time we spend on the internet, we need strong safeguards. Because if we don't protect our data, our technological systems will come to an end.

The biggest risk facing our internet system is cybercrime. The frequency of cybercrime is randomly rising every day. Every day, the US National Security Agency (NSA) receives 300 million hacking attempts. In addition, six million dollars Facebook accounts are compromised daily. The root cause of problems in our global village is hacking. It affects the entire planet and is not a problem specific to any one nation. (Billion Dollar Heist, 2023)

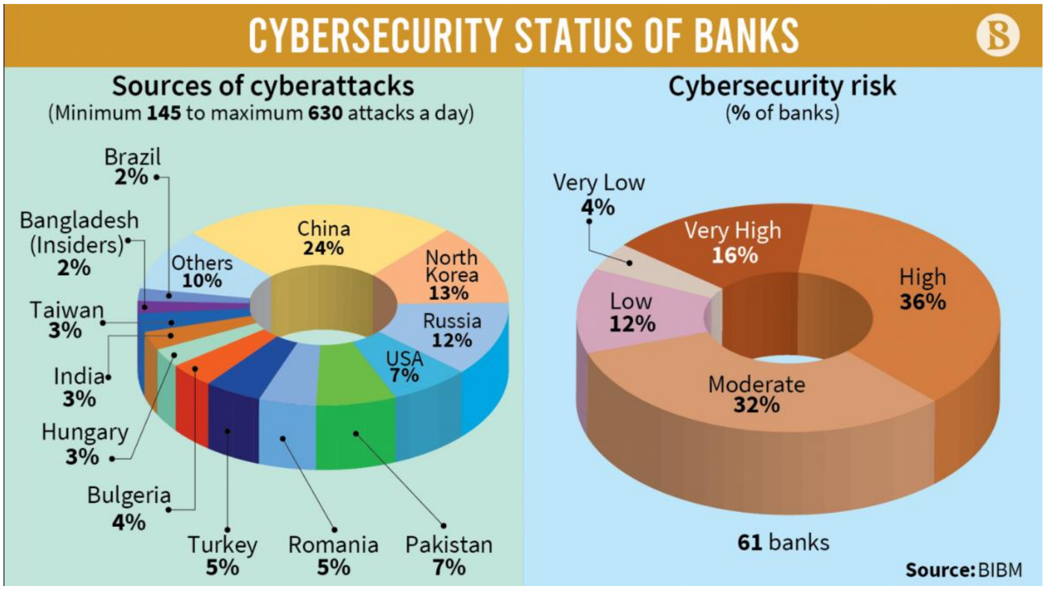


Figure 1: Cybersecurity Status of Banks (Md Mahbubur Rahman Alam, 2022)

The hacking of a bank account in Bangladesh serves as a basic example of the harm that cybercrime poses to global trade. Our digital business struggles with hacking attempts on a daily basis. In addition to all security procedures, banks are in charge of their own personal cyber security. This is the area where system vulnerabilities are being exploited by hackers. For example, smaller banks in less developed and poorer countries with inadequate cyber security systems and procedures have been the subject of successful attacks by the hacker group Lazarus. It is believed that Bangladesh Bank may have used insider information to enable the attack to succeed. (Bergman, May 13, 2021)

Figure 2: Bangladesh Bank Logo

Figure 3: Bangladesh Bank

1.2. Technical Terminologies

- Spear Phishing

  Spear phishing is a targeted cyberattack that targets particular people or companies. Spear phishing carefully selects victims, compared with massive phishing operations that infect inboxes with general offers. Attackers prepare by carefully gathering information about their targets. Social media profiles, business websites, and even trade journals may provide this information. Equipped with this information, they build emails that seem to come from a trustworthy source, such as a manager, colleague, or well-known business.

- Fake TLS Protocol

  The term "Fake TLS" describes a method used by attackers for hiding their malicious actions, even though there isn't an actual Fake TLS protocol. The first handshake of the genuine Transport Layer Security (TLS) protocol, which encrypts data transmission between devices, is copied by fake TLS. This gives the appearance of a safe connection.

- Backdoor

  In the field of cybersecurity, a backdoor is simply a secret gateway that gets passed standard security safeguards. Consider a highly guarded, alarm-equipped structure with sealed doors and guards. A backdoor function similarly to a secret gateway that a criminal could use to enter undetected.

- File Wiper

  A file wiper, sometimes referred to as a file shredder, is a digital security tool that can remove files from your computer's storage permanently. A file wiper replaces the deleted file's location on the storage disk with random data, as opposed to just deleting a file and emptying the recycle bin, which doesn't actually remove the data.

- SWIFT – DRIDEX

  A specific kind of malware known as SWIFT - DRIDEX targets the SWIFT banking network, which is used frequently across the world for financial transactions. A particular kind of banking Trojan called DRIDEX is made to take private data—especially banking credentials—from compromised systems. The malware gains even more power when paired with SWIFT since it can penetrate the safe network that banks use to send money across borders. Because it can result in scams and unauthorized access to accounts, this combination poses a serious threat to financial institutions. The DRIDEX – SWIFT malware highlights the continuous difficulty with cybersecurity in the banking industry and the necessity of strong defenses against more complex cyberattacks.

1.3. Aims and objective

The main aim of this report is to understand the attack that happened with Bangladesh bank in 2015-2016

- To research into the apt attack on Bangladesh bank.
- To research on all the events that occurred while attacker attacked the bank and present all the malware, tools and techniques used by the attackers.
- As a Chief Information Security Officer what things need to be implemented in plans and preventative actions for the bank to prevent future losses.

2. Section - 1

2.1. What and how it happened?

The February 2016 cyberattack that targeted Bangladesh's central bank was a highly skilled theft that took use of multiple weaknesses. This is a thorough account of what happened, highlighting the strategy used by the attackers and the bank's response:
A printer problem at the Bangladesh Bank on February 4th went undiscovered since it was thought to be a small glitch. This printer was not functioning until Sunday, February 7th, when IT staff finally resolved the issue. Normally, this printer prints a record of real-time transactions. After repairing the printer and restarting the system, a quick series of transactions started to print, which caused the director and staff to become concerned. A closer look turned up 35 doubtful payment requests for large amounts that were sent to several international accounts from Bangladesh Bank's private account. The fact that these transfers were made without permission was the most worrying factor. The military-grade security of the officially "unhackable" SWIFT security system was also compromised. Upon multiple tries to log in, an error message indicating that a file was missing or changed appeared. The bank director's awareness of the complete scope of the attack was temporarily delayed by this technological barrier. Later investigations uncovered an important detail: one month before the heist, a bank employee had unintentionally opened a malicious email disguised as an official one. This software created a backdoor in the bank's network, giving the attackers access without authorization. The intruders carefully observed the procedures and workings of the bank for a month without being noticed. (Billion Dollar Heist, 2023)

The attackers used the compromised system one last time on February 4. They started making fake payments through the SWIFT network by using the credentials that were stolen by the malware. These payments seemed to be real since they came directly from the bank. On investigation of the transactions, it was discovered that Bangladesh Bank had an account at the Federal Reserve Bank of New York, where it was processing 35 transfer requests worth a shocking $951 million. The attackers most likely chose this particular bank as their target because of the easily accessible cash for cross-border settlements. The goal of these transfers was to move money from New York to other Asian accounts. fortunately, the Federal Reserve Bank in New York identified thirty of the transfer requests for manual review on Friday, February 5. This lucky incidence resulted from one shipping firm name that was accidentally included in one of the SWIFT orders and was blocked. Because of the continuing political tensions between the United States and Iran, this name set off an alarm. As a result, $871 million worth of transfers were stopped. (digiALERT, 2023)

Although some transfers were partially blocked, Bangladesh Bank still had to deal with other issues. The last transfer went through a German bank and was made to an NGO in Sri Lanka. Luckily, the $20 million payment was detected by the German bank because the recipient's name was spelt "**Fandation**" rather than "**Foundation**" Furthermore, the intended recipient, Pan Asia Bank in Sri Lanka, returned the transaction to the German bank for verification due to their suspicions regarding the high sum. Bangladesh Bank might have been able to get this money back as a result of the delay. The remaining four transactions, which were made to a Philippine bank, could not be located. The attack occurred during the Chinese New Year holiday in the Philippines, giving the attackers a window of opportunity. It was almost impossible to collect the stolen money because it was quickly turned into cash and cleaned through casinos. This analysis highlights the attackers' careful preparation, which included using malware, credentials that had been stolen, and a well-timed strike around the holidays. Bangladesh Bank was lucky to recover some money, but the incident also revealed serious weaknesses in the SWIFT network and the bank's security procedures. It is an eye-opening indicator of how advanced cyberattacks are becoming and how crucial it is for financial institutions to have strong cybersecurity defenses in place. (Das & Spicer, 2016), (Billion Dollar Heist, 2023)

2.2. Possible Flaws of the Bangladesh Bank:

- It's possible that security updates haven't been applied to undiscovered vulnerabilities in the bank's network. (Billion Dollar Heist, 2023)
- It's possible that two-factor authentication was not used for SWIFT transactions, which would have allowed for illegal access using credentials that were stolen. (Billion Dollar Heist, 2023)
- Though unverified, there have been rumours of potential insider participation within the bank or the SWIFT network. (Bergman, May 13, 2021)
- It's possible that insufficient processes for examining and approving big transactions prevented the false transfers from being discovered. (digiALERT, 2023)

Tools	Uses
Spear Phishing	To get initial access to the bank's network. Used C.V in the mail with malicious link.
Command and Control	To direct and control the bank system using a backdoor which is embedded through phishing.
SWIFT- DRIDEX	This malware helped them in sending fraudulent payment requests by tampering SWIFT responses. (Bergman, May 13, 2021)
Fake TLS Protocol	This protocol used to duplicate TLS traffic to bypass network security measures.
Secure File Wiper	It helps the attacker to erase all traces.
Backdoor	A method that allows unauthorized access to a computer system, network, or software application. (Das & Spicer, 2016)
Money Laundering	They transferred the money by making transaction through Philippine bank and by playing in a casino. (Billion Dollar Heist, 2023)

Table 1: Tools and Techniques used in the attack

2.3. Timeline of the Bangladesh bank attack:

Early 2015:

- According to the NSA, it appears that attackers might have started spying on Bangladesh Bank during this time. (PAZ, 2016)

May 15th, 2015:

- In a Philippine branch of the Rizal Commercial Banking Corporation (RCBC), three fake bank accounts are opened. These accounts, which are later connected to the stole money, are inactive as of February 4, 2016. (Trove, 2019)

Feb 4th, 2016:

- Hackers breach Bangladesh Bank's network by taking advantage of unknown vulnerabilities.
- Systems that handle and approve financial transactions get infected with malware. Probably, this malware infection gave hackers a way to change data or steal credentials.
- The login credentials for Bangladesh Bank's SWIFT terminal, the platform used for international money transfers have been successfully hacked by attackers. (Trove, 2019)

Feb 4th-5th,2016:

- Attackers use the credentials they extracted to send fake transfer requests across the SWIFT network. Approximately $951 million is being requested to be transferred to other accounts across the globe, with the majority going to the RCBC accounts in the Philippines. (Trove, 2019)

Feb 6th, 2016:

- Receiving banks report likely attempted transactions as suspicious, which keeps them from getting done. However, a number of transfers totaling about $81 million are managed successfully and end up in the Philippines' RCBC accounts.
- After discovering of the false transfers, Bangladesh Bank alerts SWIFT to the situation. (PAZ, 2016)

Feb 9th, 2016:

- Despite an instruction for a proper inquiry and a SWIFT code from Bangladesh Bank asking refunds or freezes, the RCBC Jupiter branch allowed $58.15 million in withdrawals from accounts. (PAZ, 2016)

Feb 29th, 2016:

- Reports from Philippine press agencies make the news of the Bangladesh Bank attack public. (Trove, 2019)

March 8th, 2016:

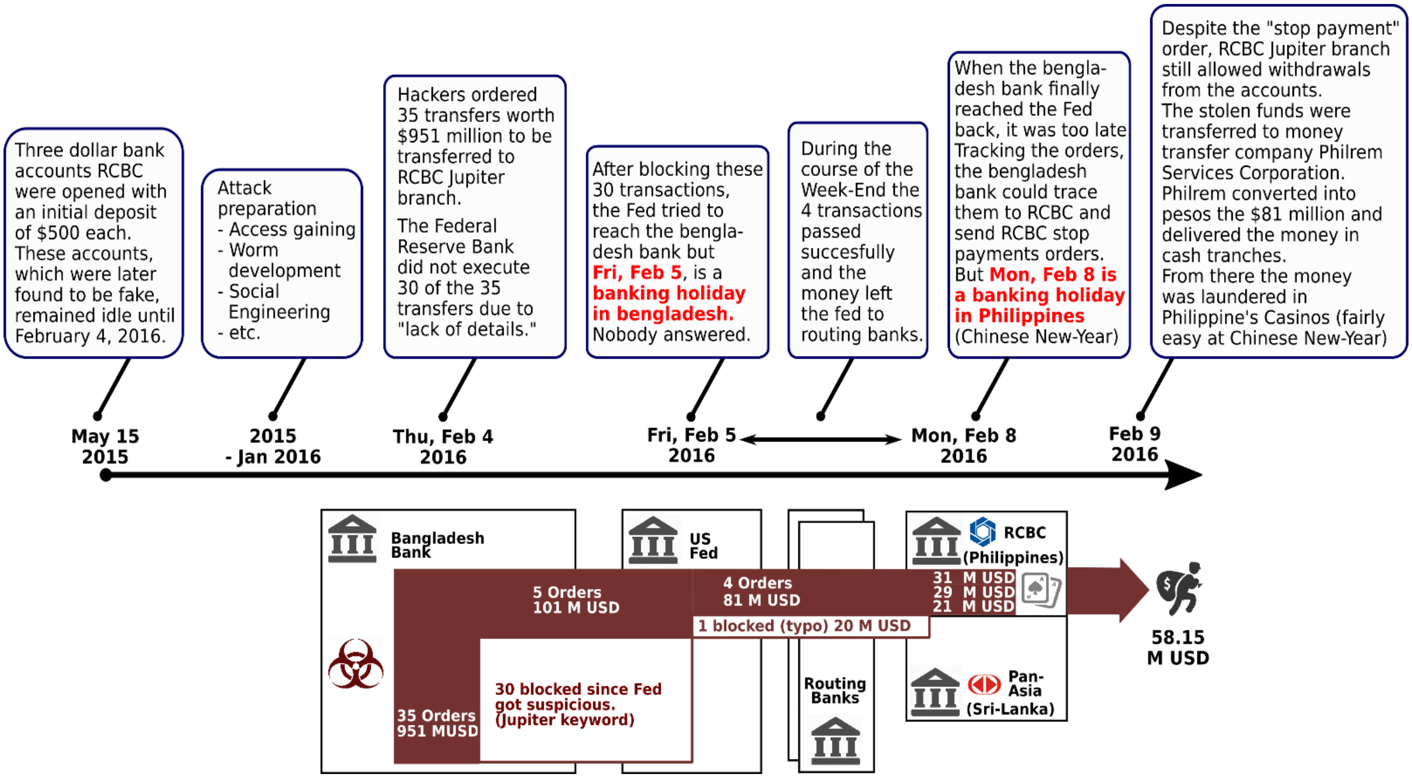
- In light of the Bangladesh Bank incident, SWIFT sends an emergency alert to its member banks, asking them to examine and improve their cybersecurity procedures. (Trove, 2019)

March 15th, 2016:

- Investigations on RCBC's contribution to the money laundering of stolen money are started by the Philippine Senate. (PAZ, 2016)

March 21st,2016:

- SWIFT encourages member banks to strengthen their local security procedures by sending them a written advice and by starting communication with them. (PAZ, 2016)



Three dollar bank accounts RCBC were opened with an initial deposit of $500 each. These accounts, which were later found to be fake, remained idle until February 4, 2016.

Attack preparation
- Access gaining
- Worm development
- Social Engineering
- etc.

Hackers ordered 35 transfers worth $951 million to be transferred to RCBC Jupiter branch.

The Federal Reserve Bank did not execute 30 of the 35 transfers due to "lack of details."

After blocking these 30 transactions, the Fed tried to reach the bangladesh bank but **Fri, Feb 5**, is a **banking holiday in bengladesh.** Nobody answered.

During the course of the Week-End the 4 transactions passed succesfully and the money left the fed to routing banks.

When the bangladesh bank finally reached the Fed back, it was too late Tracking the orders, the bengladesh bank could trace them to RCBC and send RCBC stop payments orders. But **Mon, Feb 8 is a banking holiday in Philippines** (Chinese New-Year)

Despite the "stop payment" order, RCBC Jupiter branch still allowed withdrawals from the accounts. The stolen funds were transferred to money transfer company Philrem Services Corporation. Philrem converted into pesos the $81 million and delivered the money in cash tranches. From there the money was laundered in Philippine's Casinos (fairly easy at Chinese New-Year)

Figure 4: Timeline of the attack (Kehrli, Nov 15, 2017)

3. Section – 2

3.1. After the attack

Bangladesh bank have to take immediate action to contain the damage, recover systems and by making strong BCP they need to be prepared from the future attacks. Firstly, they need to inform the cybersecurity officer or organization so they can block the attack and they also need to inform their respective customers not to use their services until they drop another notice. After they known to that attack has happened at the bank, they need disconnect all compromised system from the network to prevent the attack which is spreading in the system. So that they can save other system inaccessible by the attackers. After that they need to protect logs, files and other data that might be helpful for the security officer while doing investigation and also helps to identify the location and the attacker as well. (Das & Spicer, 2016)

Secondly, they need to activate the bank's BCP if there is and find the root cause of the attack and start with steps mentioned in the BCP. After that they need to inform the relevant authorities to handle the problem including security cell of the bank and law enforcement agencies. They need to understand how it happened, what was the root cause and vulnerabilities in their system. They need to figure out the how much data had been stolen by the attacker and how important was that and try to recover them accordingly. Bank need to inform their respective customer about the attack, the impact of the attack and steps they need to take while using their service if necessary.

Hackers used the SWIFT terminal, which is a system used by many banks worldwide to communicate financial transfers, to target the central bank of Bangladesh. The SWIFT system has faults that might be used by hackers to acquire passwords and send false transfer messages, as shown by this amazing cyber theft. The attack highlights the value of strong security procedures across the board for an organization and the dangers of connecting third-party systems into vital financial operations. (Billion Dollar Heist, 2023),

4. Section – 3

4.1. If I were the CISO,

I will work accordingly to the following's points.

4.1.1. Immediate Action:

If I were the CISO of the Bangladesh Bank, I will first isolate all compromised systems which are connected in the network to prevent the attackers from the moving laterally and accessing more systems. To stop more false transfers, I will stop all outgoing financial transactions, especially those that were started using the SWIFT terminal. Then I will try to secure logs, server data and other information which could be useful for forensic study and to track the identity of the attacker.

4.1.2. Communication and Alerting:

Contact an emergency response team immediately, including important members from operations, security, and IT. Make sure everyone is aware of the problem and turn on the bank's incident response plan. Inform appropriate authorities, such as law enforcement and the Bangladesh Bank Cyber Security Cell. This makes it possible to coordinate an investigation and maybe identify the attackers. Report the attack to SWIFT as soon as you can. They are able to monitor the scams and maybe notify other institutions that are involved as a consequence. Work with bank and SWIFT to find and stop any illegal payments that are still being processed. Identify any vulnerabilities that the attackers exploited while trying to contain the attack. Later on, this will be essential for putting in place enhanced safety measures. If social engineering was a part of the assault, inform staff members right away about phishing scams and other attack strategies.

4.2. Safety Measures:

4.2.1. Improved Internal Security:

- Add a second verification factor to passwords for all access points, including the SWIFT terminal, using Multi-factor Authentication (MFA).
- Split the network into segments to keep important systems, such as SWIFT, apart from other areas of the bank's network. If one system is hacked, the damage is limited as a consequence of the breach.
- Update software and systems frequently with the newest security patches to fix vulnerabilities.
- Establish a system of stronger access controls, allowing access to only those necessary required for each user's function. This reduces the possibility of unwanted entry.
- Train staff members on safe password management, how to spot phishing scams, and how to report suspicious behavior.

4.2.2. SWIFT Security

- Increase the implementation of enhanced two-factor authentication on the SWIFT network to further secure financial transactions.
- Establish stronger transaction monitoring procedures together with SWIFT to spot issues and possibly unauthorized activities.

4.2.3. Third-Party Risk Management:

- Carry out full security assessments of any outside suppliers or platforms such as the shared payment platform and other systems or organization which are linked to the bank's systems.
- Make sure third-party providers follow strict security procedures by include strong security terms in their contracts (tt, 2122).

5. Conclusion

Nearly $1 billion in public funds were stolen from Bangladesh Bank, an amount of money for a third-world nation like Bangladesh. It's difficult to say if the money was intentionally laundered through authorized organizations or if it was just a lucky break, but being exposed at Deutsche Bank and New York Band saved about 90% of the total. It's also important to note that the malware persisted on the Bank's network for a considerable amount of time, taking its full time. Unknown hackers utilized this time to plot and coordinate their attack on the bank. Although practically all financial institutions in the world use the SWIFT network, which is thought to be safe, in this case it was used as an opening for an attack. A good example of the saying "the chain is as strong as its weakest link" could be this. Getting protective cybersecurity technology is important these days, but it's also crucial to invest in cybersecurity knowledge and procedures and train human resources in them. This is because, despite the state-of-the-art nature of the technology, it is still operated by prone to error human beings.

6. References

Das , K. N. & Spicer, J., 2016. *How the New York Fed fumbled over the Bangladesh Bank cyber-heist.* [Online]
Available at: https://www.reuters.com/investigates/special-report/cyber-heist-federal/
[Accessed 1 April 2024].

PAZ, C. D., 2016. *TIMELINE: Tracing the $81-million stolen fund from Bangladesh Bank.* [Online]
Available at: https://www.rappler.com/business/industries/125999-timeline-money-laundering-bangladesh-bank/#:~:text=February%204%2C%202016%20%E2%80%93%20Hackers%20broke,transferred%20to%20RCBC%20Jupiter%20branch.&text=But%20the%20remaining%20%2481%2Dmillion,fake%20bank
[Accessed 1 April 2024].

Bergman, D., May 13, 2021. *How Bangladesh Bank was hacked.* [Online]
Available at: https://medium.com/netranews/how-bangladesh-bank-was-hacked-12714bd089b5
[Accessed 31 March 2024].

Billion Dollar Heist. 2023. [Film] Directed by Daniel Gordon, Brendan Donovan. United States of America: Billion Dollar Heist.

digiALERT, 2023. *Case Study on Bangladesh Banking Heist.* [Online]
Available at: https://www.linkedin.com/pulse/case-study-bangladesh-banking-heist-digialert/
[Accessed 31 March 2024].

Kehrli, J., Nov 15, 2017. *Deciphering the Bangladesh bank heist.* [Online]
Available at: https://www.niceideas.ch/roller2/badtrash/entry/deciphering-the-bengladesh-bank-heist
[Accessed 2 April 2024].

Md Mahbubur Rahman Alam, 2022. *Majority of banks at high cyber risks: BIBM study.* [Online]

Available at: https://www.tbsnews.net/economy/banking/majority-banks-high-cyber-risks-bibm-study-438594
[Accessed 2 April 2024].

Trove, T., 2019. *BANGLADESH BANK ROBBERY TIMELINE.* [Online] Available at: https://nsarchive.gwu.edu/news/cyber-vault/2019-02-20/tainted-trove
[Accessed 1 April 2024].

tt, 2122. *tt.* [Online].

7. Appendix

7.1. SWIFT

The organizing body of safe international money transfers is the Society for Worldwide Interbank Financial Telecommunication, which is also known as **SWIFT**. It's just a chat app designed for banks. Banks can send and receive information for transactions like trades and payments fast and correctly thanks to this worldwide network. Though it doesn't manage the money directly, SWIFT makes sure these messages are secure and understandable. Additionally, they give banks different codes think of it as a worldwide address book for finance. International financial transactions for both personal and business purposes may run smoothly with SWIFT, all because of this secure messaging technology.

Full Form of SWIFT
S.W.I.F.T.
Society for Worldwide Inter-Bank Financial Telecommunication
WallStreetMojo

Figure 5: SWIFT

7.2. Lazarus

The Lazarus Group, a notorious hacking group allegedly backed by North Korea, has been a thorn in the side of cybersecurity for over a decade. With the goal of causing disruption, stealing, or spying, they have targeted anything from financial organizations like Bangladesh's central bank to entertainment firms like Sony Pictures. Lazarus uses a variety of clever strategies, such as social engineering and zero-day exploits, to obtain access; they frequently cover their tracks by raising false alarms. Their financial goals have changed to involve massive bitcoin thefts that result in large losses. The Lazarus Group is still one of the biggest threats to cybersecurity because of its aggressive tactics and flexibility.

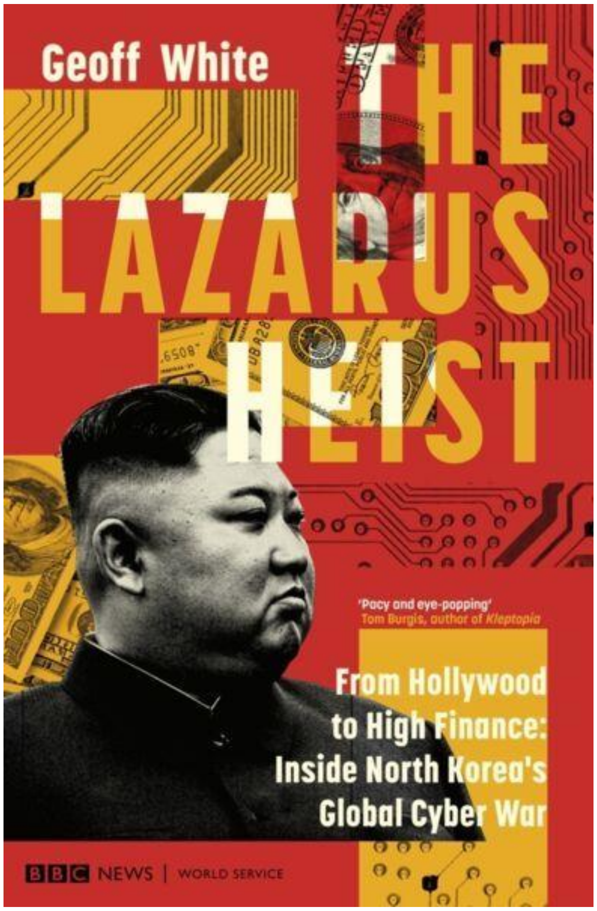

Geoff White
THE LAZARUS HEIST
'Pacy and eye-popping'
Tom Burgis, author of Kleptopia
From Hollywood to High Finance: Inside North Korea's Global Cyber War
BBC NEWS | WORLD SERVICE

Figure 6: Lazarus Group