CASE STUDY:

COLONIAL GAS PIPELINE RANSOMWARE ATTACK
&
BANGLADESH BANK ROBBERY

PRESENTED BY:

PRIYANKA KUMARI

CONTENTS:

CASE STUDY - 1:

Colonial Gas Pipeline Ransomware Attack (2021)

INTRODUCTION

The Colonial Pipeline ransomware attack was a significant cyberattack that occurred on May 7, 2021. The attack targeted Colonial Pipeline, the largest fuel pipeline in the U.S., which transports gasoline, diesel, and jet fuel from Texas to the East Coast.

KEY POINTS:

- **Largest U.S. Fuel Pipeline**
  The Colonial Pipeline spans over **5,500 miles** from Texas to New Jersey. It is a crucial part of the U.S. energy infrastructure, carrying massive quantities of fuel to various states, ensuring that millions of consumers, businesses, and industries receive the energy they need for transportation, manufacturing, and daily use.

- **East Coast Fuel Supplier**
  The pipeline is responsible for supplying nearly **45% of the East Coast's fuel needs**, including gasoline, diesel, and jet fuel. This makes it a critical artery for the energy sector, providing fuel to densely populated and industrially significant areas.

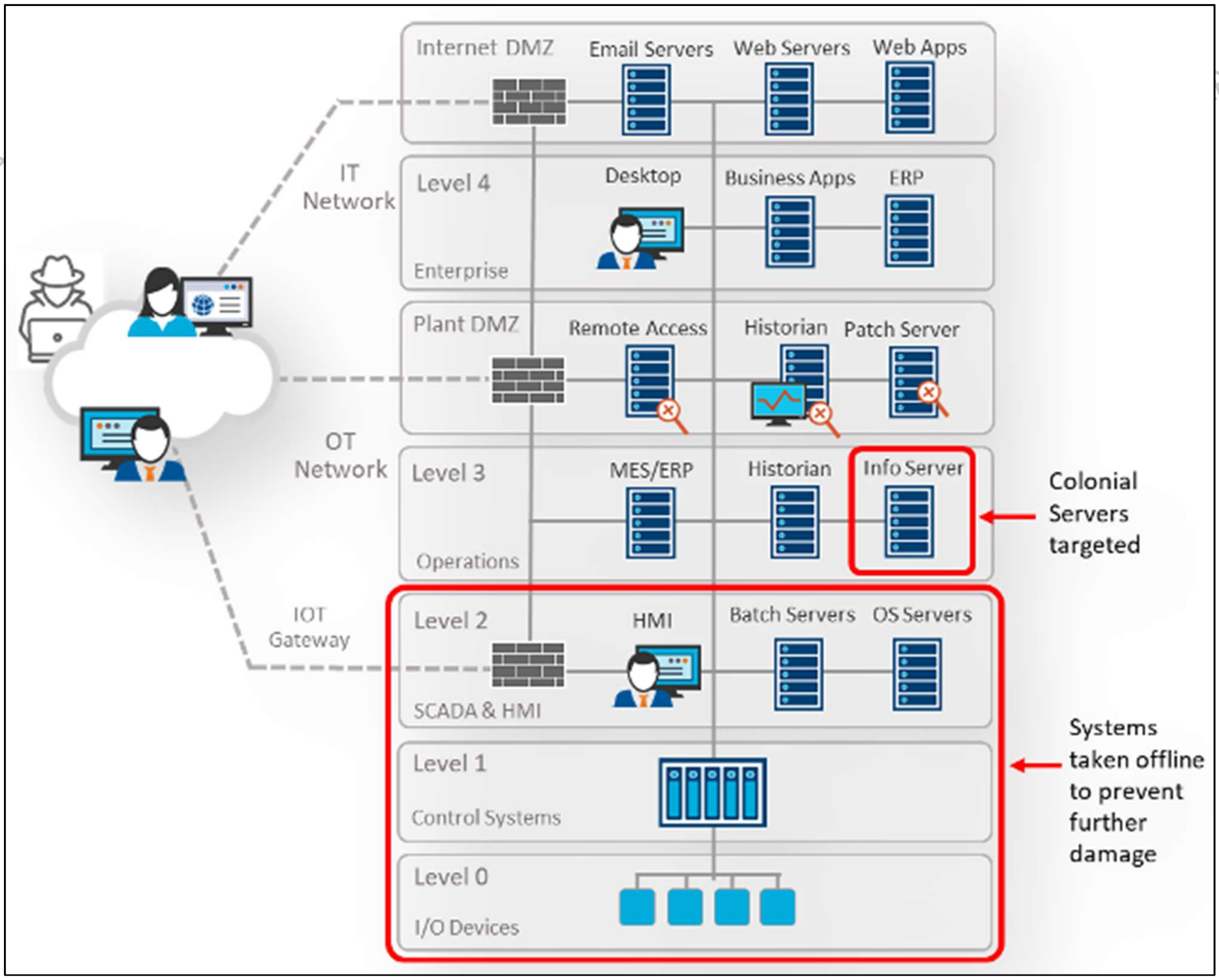
- **Critical Infrastructure**
  As one of the most important pieces of U.S. energy infrastructure, the Colonial Pipeline is classified as **critical**. Its smooth operation is essential for national energy distribution, affecting the economy, transportation, and energy security across the Eastern U.S.

- **High Cyberattack Risk**
  Due to its immense strategic importance, the Colonial Pipeline is a **prime target** for cyberattacks. The ransomware attack exposed vulnerabilities in the energy sector and highlighted the urgent need for stronger cybersecurity measures to protect key infrastructure from similar threats in the future.

IDENTIFYING THE PERPETRATORS

- **Perpetrators:** The ransomware group Dark Side, a cybercriminal organization, was responsible. They employed ransomware to lock Colonial Pipeline's IT systems and demanded a ransom payment in exchange for decryption.

- **Method:** The attack involved phishing and exploiting vulnerabilities in Colonial's network security, leading to the encryption of key business systems.



ANALYSIS OF COLONIAL GAS PIPELINE CYBER ATTACK

ATTACK SEQUENCE

1. **Infiltration:**
   The exact entry method is unclear, but possibilities include phishing, insider threats, remote access, or exploiting vulnerabilities.

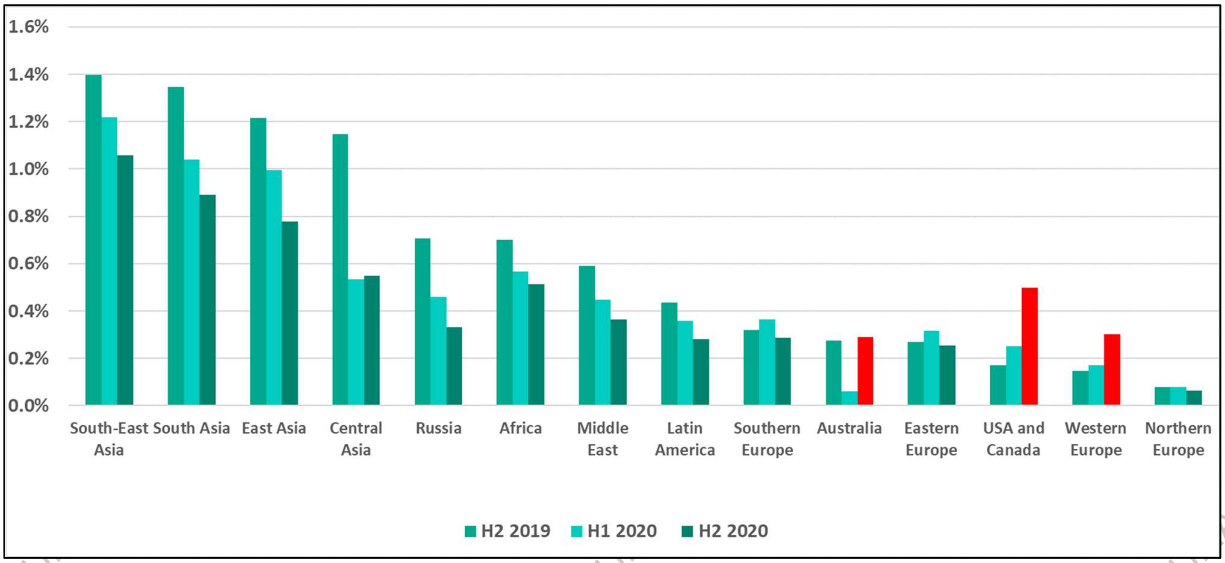
2. **Malware:**
   Dark Side is a compressed executable using RSA 1024 and Salsa20 encryption. The ransom note, victim GUID, and C2 server addresses are stored in a compressed file.

3. **First Execution:**
   The malware:
   - ✓ Resolves library calls and decrypts strings.
   - ✓ Loads necessary libraries and checks privileges.
   - ✓ Uses UAC elevation if needed, adjusts token privileges, and mimics the user's context.
   - ✓ Creates a unique checksum, logs actions, and ensures only one instance runs.
   - ✓ Exits if the system language is Russian.

4. **Encryption Stage:**
   The malware checks disk space, contacts the C2 server, and identifies the victim using a unique hash. It deletes shadow copies, terminates processes, and encrypts files across local and network shares. Encrypted files are exfiltrated before the malware deletes itself.

5. **Virsec's Protection:**
   Virsec's AppMap® technology detects and stops attacks in real-time by preventing unauthorized execution deviations. It could have intercepted the attack early and stopped it at multiple stages.

IMPACT OF THE ATTACK



Percentage of ICS computers on which ransomware was blocked, H2 2019-H2 2020

- **Operational Disruption:** Colonial Pipeline shut down its operations for nearly a week to contain the breach, leading to widespread fuel shortages, panic buying, and price increases across the East Coast.

- **Economic Consequences:** The disruption affected airlines, transportation sectors, and consumers. Gas prices surged to their highest levels since 2014.

- **Ransom Payment:** Colonial Pipeline paid a ransom of approximately $4.4 million in Bitcoin. However, a portion of the payment was later recovered by the U.S. Department of Justice.

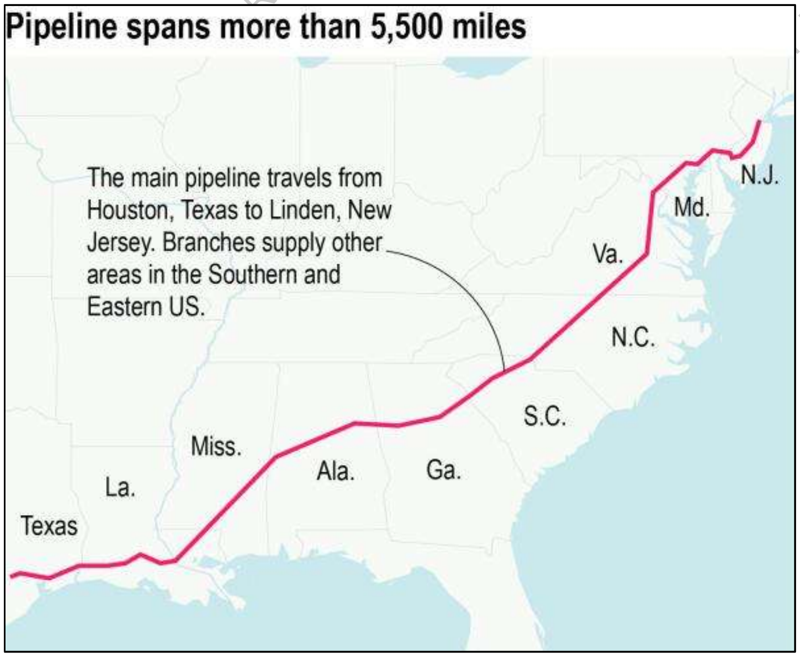
- **Catalyst for Policy Change:** The attack served as a wake-up call for both the private sector and government, catalyzing discussions around enhancing national cybersecurity policies. It led to increased scrutiny and new initiatives focused on safeguarding critical infrastructure, reflecting a broader recognition of the need for robust defenses against emerging cyber threats.

GOVERNMENT AND INDUSTRY RESPONSE

- **Emergency Declarations:** The U.S. government declared a state of emergency in response to the fuel shortages.

- **Strengthened Cybersecurity:** The attack highlighted vulnerabilities in critical infrastructure, prompting increased investment and regulations to bolster cybersecurity standards for utilities and other essential sectors.

- **National Security Reevaluation:** The incident led to a reevaluation of national security priorities concerning cybersecurity, emphasizing the need for a unified strategy to safeguard critical infrastructure. This prompted enhanced collaboration among federal agencies, private sector stakeholders, and cybersecurity experts to build a more resilient defense against future attacks.


Pipeline spans more than 5,500 miles
The main pipeline travels from Houston, Texas to Linden, New Jersey. Branches supply other areas in the Southern and Eastern US.
N.J.
Md.
Va.
N.C.
S.C.
Ga.
Ala.
Miss.
La.
Texas

COLONIAL PIPELINE SYSTEM

LESSONS LEARNED

- **Critical Infrastructure Protection**
  Critical infrastructure is a prime target for hackers, posing business, safety, and national security risks. The Colonial Pipeline attack highlighted the need for private-public collaboration in cybersecurity. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 mandates reporting cyber incidents to CISA, aiding in trend analysis and victim support.

- **Ransom Payment Dilemma**
  Paying ransoms may expedite recovery but poses risks: no guarantee of decryption, incentivizing future attacks, and potential legal issues. Businesses should involve authorities like the FBI, and maintain backups to reduce hacker leverage.

- **Cyber Hygiene and Access Control**
  The attack exploited a single password, lacking MFA. Strong cyber hygiene practices like MFA, password management, and network segmentation can prevent breaches.

- **Incident Response Plan Importance**
  A well-prepared incident response plan is crucial. It should detail scenarios, maintain functions, define responsibilities, and include communication protocols. Regular reviews and exercises can improve the plan’s effectiveness.

- **Insurance Coverage**
  Cyber insurance is essential to mitigate financial impacts. Businesses should consult experts to secure adequate coverage

CONCLUSION

The Colonial Pipeline ransomware attack served as a stark wake-up call, exposing significant vulnerabilities within the nation's critical infrastructure. This incident highlighted how susceptible essential services are to cyber threats, prompting immediate attention from both industry leaders and government officials.

As a result, there was a concerted push for significant changes in cybersecurity practices across various sectors. Organizations began to prioritize the implementation of more robust security measures, such as advanced threat detection systems, regular security audits, and employee training programs to enhance awareness about cyber hygiene.

In parallel, the attack spurred changes in government policies aimed at strengthening national cybersecurity frameworks. Federal agencies-initiated collaborations with private sector partners to develop standardized protocols for incident response and reporting. Additionally, new legislation was introduced to mandate cybersecurity risk assessments for critical infrastructure providers, ensuring they adhere to strict safety protocols.

Furthermore, the incident fostered greater public awareness about the implications of cyber threats on everyday life. Community outreach programs were launched to educate citizens about the importance of cybersecurity and the role they play in protecting essential services. Overall, the Colonial Pipeline attack catalyzed a more proactive approach to cybersecurity, emphasizing resilience and preparedness against future threats.

REFERENCES

- "Colonial Pipeline Ransomware Attack." *Insurica*, https://insurica.com/blog/colonial-pipeline-ransomware-attack/.

- *The Guardian*. "Colonial Pipeline Shutdown: Hackers' DarkSide Message to US." 10 May 2021, https://www.theguardian.com/us-news/2021/may/10/colonial-pipeline-shutdown-us-darkside-message.

- "Cybersecurity Attack Shuts Down a Top U.S. Gasoline Pipeline." *NPR*, 8 May 2021, https://www.npr.org/2021/05/08/995040240/cybersecurity-attack-shuts-down-a-top-u-s-gasoline-pipeline.

- Mehrotra, Kartikay, and Michael Riley. "Colonial Hackers Stole Data Thursday Ahead of Pipeline Shutdown." *Bloomberg*, 9 May 2021, https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown.

- Morrow, Allison (May 22, 2021). “A crypto crash wiped out $1 trillion this week. Here's what happened | CNN Business" *CNN*. https://edition.cnn.com/2021/05/22/investing/crypto-crash-bitcoin-regulation/index.html

CASE STUDY - 2:

Bangladesh Bank Robbery (2016)

INTRODUCTION

The Bangladesh Bank robbery in February 2016 involved a sophisticated cyberattack where hackers stole $81 million from the central bank's account at the Federal Reserve Bank of New York. The heist is notable for its scale and the vulnerabilities it exposed in the global financial system.

- **Timeline of the attack**
  - **Date**: February 4-5, 2016
  - **Amount Targeted**: $951 million
  - **Amount Stolen**: $81 million

KEY POINTS:

- **Overview of Bangladesh Bank**
  The Bangladesh Bank, established in 1972, serves as the country's central bank, overseeing monetary policy and financial regulation. It manages foreign reserves and plays a critical role in the nation's economy.

- **Exploitation of SWIFT System**
  Hackers accessed Bangladesh Bank's SWIFT network to send fraudulent transfer requests, ultimately stealing $81 million from its account at the Federal Reserve Bank of New York.

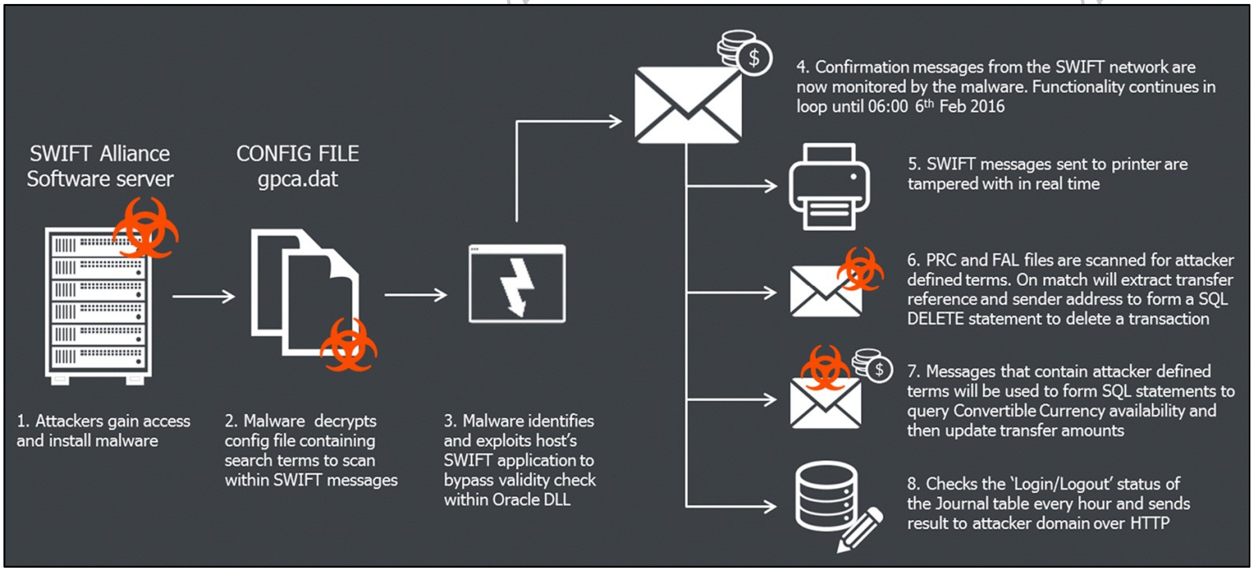
- **Cybersecurity Vulnerabilities**
  The incident revealed significant weaknesses in the cybersecurity measures of financial institutions, especially regarding their reliance on legacy systems and inadequate security protocols.

- **Global Regulatory Response**
  The robbery prompted increased scrutiny and discussions among regulatory bodies worldwide about enhancing cybersecurity practices, improving international collaboration, and establishing stronger security standards in the banking sector.

DETAILS

- **Destination and Laundering**:
  The stolen funds were routed to four accounts at RCBC (Rizal Commercial Banking Corporation) in the Philippines. The money was quickly withdrawn and laundered through the Philippine casino industry, which had weak anti-money laundering controls, making it difficult to trace and recover the funds.

- **Error Prevention**:
  A typographical error in one of the fraudulent transfer requests, where "foundation" was misspelled as "fandation," triggered suspicion at the Federal Reserve Bank. This error helped block further transactions, preventing the hackers from stealing the full $951 million.


SWIFT Alliance Software server
CONFIG FILE gpca.dat
1. Attackers gain access and install malware
2. Malware decrypts config file containing search terms to scan within SWIFT messages
3. Malware identifies and exploits host's SWIFT application to bypass validity check within Oracle DLL
4. Confirmation messages from the SWIFT network are now monitored by the malware. Functionality continues in loop until 06:00 6th Feb 2016
5. SWIFT messages sent to printer are tampered with in real time
6. PRC and FAL files are scanned for attacker defined terms. On match will extract transfer reference and sender address to form a SQL DELETE statement to delete a transaction
7. Messages that contain attacker defined terms will be used to form SQL statements to query Convertible Currency availability and then update transfer amounts
8. Checks the 'Login/Logout' status of the Journal table every hour and sends result to attacker domain over HTTP

BANGLADESH BANK HEIST GANG USED A MALWARE AND COULD STRIKE AGAIN

MALWARE ATTACK SEQUENCE

1. **Spear-phishing**
   Hackers sent emails to Bangladesh Bank employees with malicious attachments or links, deceiving them into opening the files.

2. **Network Access**
   Through these emails, hackers gained unauthorized access to the bank's computer systems, including payment transfer credentials.

3. **SWIFT Exploitation**
   Hackers manipulated the SWIFT system (Society for Worldwide Interbank Financial Telecommunication) to initiate unauthorized transfers.

4. **Fraudulent Requests**
   Using stolen credentials, the hackers sent fraudulent transfer requests to the Federal Reserve Bank of New York.

5. **Approved Transfers**
   Several requests were approved, including $20 million to Sri Lanka and $81 million to the Philippines.

6. **Incomplete Transfers**
   Only five transactions were processed; incomplete information halted the others.

THE FEDERAL RESERVE BANK OF NEW YORK BUILDING

INVESTIGATION AND IMPACT

- **Suspected Perpetrators**: The Lazarus Group, a North Korean hacking organization, is suspected due to similar attack patterns.

- **Recovery**: Approximately $15 million of the stolen funds were recovered. The rest was lost through the casino industry in the Philippines.

- **Global Impact**: The heist highlighted weaknesses in SWIFT's security and led to enhanced cybersecurity measures and regulatory reforms, especially in anti-money laundering practices.

81M Dollar Story

Bangladesh sues Philippine bank, staff over brazen cyber heist

Investigators believe the North Koreans practiced by hitting Sony Corp. in 2014

RCBC's lead attorney challenged the lawsuit, claiming the Bangladesh Bank should be liable for its errors and lapses in security protocols

Bangladesh Bank lawsuit alleges Philippine bankers were involved in a multi-year conspiracy with North Korean hackers

The lawsuit alleges Rizal Commercial Banking Corp. (RCBC) of the Philippines along with eight bank officers conspired with casino operators, Chinese citizens and the hackers to steal the money

The 103-page complaint alleges: "The conspiracy was seamless, with every complicated step plotted out in advance"

BANGLADESH MONEY HEIST

LESSON LEARNED:

- **Cybersecurity Gaps**: Financial institutions can be vulnerable to sophisticated cyberattacks if they lack robust security measures.

- **Weak Oversight**: The lack of stringent monitoring in high-risk industries (e.g., casinos) can facilitate money laundering.

- **Importance of SWIFT Security**: Even secure systems like SWIFT can be compromised if proper protocols and monitoring are not enforced.

- **Human Oversight is Critical**: A simple typo triggered a red flag, highlighting the importance of manual review alongside automated systems.

- **Cross-Border Vulnerabilities**: Global financial systems can be exploited through cross-border transactions, especially where regulations vary widely.

- **Prevention strategies:**

  ✓ **Strengthen Cyber Defenses**: Implement multi-layered security systems, including firewalls, encryption, and regular system audit.

  ✓ **SWIFT Security Upgrades**: Ensure real-time monitoring and implement security checks on SWIFT network transactions.

  ✓ **Employee Training**: Regular training on cybersecurity awareness and protocols for detecting suspicious activity.

  ✓ **Stricter Anti-Money Laundering (AML) Laws**: Strengthen international AML regulations, particularly in sectors like casinos.

  ✓ **Global Cooperation**: Improve collaboration between banks, governments, and regulators to share intelligence on cyber threats.

CONCLUSION

The 2016 Bangladesh Bank robbery exposed critical vulnerabilities in the cybersecurity frameworks of financial institutions, particularly within the global banking system. Hackers managed to exploit weaknesses in the Bangladesh Bank's systems and the SWIFT network, leading to the unauthorized transfer of $81 million. This incident not only highlighted the immediate security flaws within Bangladesh Bank but also raised alarms about the potential for similar breaches across other financial entities worldwide.

As a result of this high-profile heist, there was a substantial push for reforms within global financial institutions. Regulatory bodies and banks began to recognize the necessity of enhancing their cybersecurity protocols to guard against increasingly sophisticated cyber threats. These reforms included implementing stricter access controls, upgrading software systems, and adopting advanced threat detection technologies.

Furthermore, the incident underscored the importance of collaboration among financial institutions, cybersecurity experts, and regulatory agencies. Sharing intelligence about potential threats and vulnerabilities became a priority to create a more resilient banking infrastructure. Training programs for employees on recognizing phishing attempts and adhering to best practices in cybersecurity also gained traction.

In summary, the Bangladesh Bank robbery served as a wake-up call for the financial sector, emphasizing the need for robust security measures. The ongoing evolution of cyber threats requires constant vigilance and adaptation to ensure the protection of sensitive financial data and the integrity of global financial systems.

REFERENCES

- "The Great Bangladesh Cyber Heist Shows Truth Is Stranger than Fiction." *Dhaka Tribune*, 1 November 2016, https://www.dhakatribune.com/opinion/op-ed/122939/the-great-bangladesh-cyber-heist-shows-truth-is. Retrieved 8 September 2024.

- Furfaro, Danielle. "Congresswoman Wants Probe of Brazen $81M Theft from New York Fed." *New York Post*, 22 March 2016, https://nypost.com/2016/03/22/congresswoman-wants-probe-of-brazen-81m-theft-from-new-york-fed/. Retrieved 8 September 2024.

- "Bangladesh Probes 2013 Hack for Links to Swift-Linked Central Bank Heist." *CNBC*, 25 May 2016, https://www.cnbc.com/2016/05/25/bangladesh-probes-2013-hack-for-links-to-swift-linked-central-bank-heist.html. Retrieved 8 September 2024.

- "Malware Used in Bangladesh Bank Heist." *ERMProtect*, https://ermprotect.com/blog/malware-bangladesh-bank-heist/#:~:text=Malware%20was%20used%20to%20monitor,in%20a%20matter%20of%20days

- Perlroth, Nicole; Corkery, Michael (26 May 2016). "North Korea Linked to Digital Attacks on Global Banks" https://www.nytimes.com/2016/05/27/business/dealbook/north-korea-linked-to-digital-thefts-from-global-banks.html?_r=0 *New York Times*