# **Title:**

Union Bank of India Cyber Heist: Navigating a $171 Million Cyberattack

# **Introduction:**

 On a seemingly ordinary Friday, July 21, 2016, Union Bank of India faced an extraordinary challenge when Chairman Arun Tiwari received a call informing him of an attempted cyber theft of $171 million from the bank's Nester account. The incident set off a chain of events, leading to a rapid response to safeguard the funds and investigate the breach.

# **Background:**

Union Bank's corporate office at Nariman Point, Mumbai, became the focal point of this cyber attack. Despite routine banking activities across numerous branches and ATMs, the tranquility of the day was disrupted by the revelation of a significant security breach that targeted the bank's Nester account.

# **Incident Overview:**

The incident involved a phishing attack initiated by an email seemingly from the Reserve Bank of India (RBI). An employee fell victim to the phishing email, triggering the release of malware that infiltrated Union Bank's servers. The attackers successfully moved $171 million through accounts in Cambodia, Thailand, Taiwan, and Australia.

# **Attack Method:**

 The attack commenced with a phishing email sent to multiple Union Bank email addresses, including customer care, e-banking, and individuals. Although some employees flagged the email as suspicious, one individual, not as tech-savvy, clicked on the link. The malware, hidden in a zip file, went viral across the bank's servers. The attackers exploited the SWIFT network to transfer funds to foreign accounts

# **Impact:**

 The attackers successfully transferred funds to accounts in Cambodia, Thailand, Taiwan, and Australia via banks like Canadian Bank Plc, RHB Indochina Bank Ltd, Siam Commercial Bank, Bank Synoptic, Citibank New York, and JP Morgan Chase New York. Union Bank detected the attack when a $170 million discrepancy appeared in the reconciliation report received from the originating bank.

# **Investigation:**

 The response involved immediate actions, including informing RBI, the ministry of external affairs, and CERT-In. Inspection and investigation were conducted by CERT-In, RBI, and Union Bank's internal team. EY, a consulting firm, was appointed for analysis and forensics. The investigation revealed that the malware originated from a phishing email with an attachment, purportedly from RBI.

# **Lessons Learned:**

Union Bank swiftly responded by delinking SWIFT connections, creating a dedicated response team, and implementing manual checks. They recovered about 70% of the funds within 24 hours and the remaining $30 million after a legal process. The incident highlighted the importance of employee awareness, rapid response, and ongoing vigilance against evolving cyber threats. Preventive measures, including stringent filtering, employee awareness, whitelisting, BIOS passwords, and engagement with regional offices, were implemented to fortify the bank's IT platform. The incident underscored the challenges in attributing cyber attacks to specific geographies and emphasised the need for constant improvement in cybersecurity measures.

# **Preventive Measures:**

 Union Bank of India implemented several preventive measures following the cyber attack:

• Strengthened employee awareness: Conducted training sessions to enhance employees' ability to identify phishing emails and suspicious attachments.

• Stringent filtering: Implemented robust email filtering systems to detect and block malicious content, reducing the likelihood of successful phishing attacks.

• Whitelisting: Utilised whitelisting, a proactive security technique, allowing only approved programs to run, preventing unauthorised access and execution of malicious code.

• BIOS passwords: Implemented BIOS passwords to enhance security by restricting external devices from accessing computers and servers.

• Centralised SWIFT operations: Delinked 380 SWIFT connections nationwide, centralising operations to streamline monitoring and control.

# **Conclusion:**

 The incident at Union Bank of India underscored the evolving and persistent nature of cyber threats in the banking sector. Despite the challenges posed by sophisticated attacks, the bank's proactive response, rapid recovery of funds, and subsequent preventive measures demonstrated resilience and a commitment to strengthening cybersecurity. The incident served as a catalyst for continuous improvement in the bank's IT infrastructure, processes, and employee awareness.

# **Recommendations:**

 Based on the lessons learned from the cyber attack, here are some recommendations for Union Bank of India and other financial institutions:

• Continuous training: Conduct regular cybersecurity training sessions to keep employees informed about the latest threats and best practices.

• Regular cybersecurity audits: Perform periodic cybersecurity audits to identify and address vulnerabilities in IT systems and processes.

• Collaboration and information sharing: Foster collaboration with industry peers and regulatory bodies to share insights, threats, and best practices in cybersecurity.

• Advanced threat detection: Invest in advanced threat detection technologies to identify and mitigate cyber threats in real-time.

• Incident response planning: Develop and regularly update incident response plans to ensure a swift and coordinated response to potential cyber attacks.

• Regulatory compliance: Stay abreast of regulatory requirements and compliance standards, implementing necessary measures to meet or exceed industry cybersecurity standards.

These recommendations aim to strengthen cybersecurity resilience, enhance collaboration within the industry, and ensure a proactive approach to mitigating the risks associated with cyber threats.

# **Note:**

Cybersecurity is an ongoing and dynamic challenge that requires constant vigilance and adaptation. The incident at Union Bank of India serves as a reminder that cyber threats can evolve rapidly, necessitating a comprehensive and proactive approach to safeguarding sensitive financial information. Financial institutions must remain committed to investing in advanced technologies, employee training, and collaborative efforts to stay ahead of cybercriminals. The lessons learned from this incident underscore the importance of a robust cybersecurity framework and the continuous pursuit of excellence in mitigating emerging cyber risks.