Government Polytechnic, Pune-16

(An Autonomous Institute of Government of Maharashtra)

A Report on

Case Study On Cyber Crimes In India: "THE ATTACK ON COSMOS COOPERATIVE BANK"

SUBMITTED BY:

1.PRERANA MHATRE (2007039)
2.JAAI PANHALE (2007047)
3.SANIYA PATHAN(2007048)

UNDER THE GUIDANCE OF

Smt. Shraddha Hande

Government Polytechnic, Pune-16

(An Autonomous Institute of Government of Maharashtra)

Department Of Information Technology

CERTIFICATE

This is to certify that **Prerana Mhatre (2007039)** Third Year Diploma in Information Technology has successfully completed the Micro project titled Case Study On Cyber Crimes In India: ”THE ATTACK ON COSMOS COOPERATIVE BANK” project as part of his diploma curriculum of Subject :- Information Security , in academic year 2022-23.

Guide	HOD	Principal
(Smt. **Shraddha Hande**)	(Smt. M.U Kokate)	(Dr. V.S Bandal)

INDEX

Abstract:

Cosmos Bank, the oldest and largest cooperative bank in India, became the victim of a cyberattack through its ATM and SWIFT payment systems in 2018. The resulting financial loss was huge. The cyberattack disrupted the digital banking services of Cosmos Bank, resulting in damage to its reputation and a significant decline in trust among its customers. The entire banking industry, especially the cooperative sector, was shaken as a result of this incident. Customers also started losing faith in digital banking channels and began to question the reliability of technology.

The chairman of the bank, Milind Kale, took strong decisive action and implemented strategies to rebuild customer trust and to enhance digital transactions. However, customers still had various apprehensions related to digital banking security at Cosmos Bank. Milind needed to implement plans with the goal of building customer trust, to both retain old customers and attract new ones. Would the existing customers be convinced to write off this cyberattack as a one-off incident? Time was short and he had to respond swiftly to these pressing dilemmas. Students will be asked to identify specific actions that would enable Milind to achieve this goal.

Brief Information:

Bank cybercrime is a growing threat in today's digital age, where financial institutions increasingly rely on technology to perform critical functions. Cybercriminals use various techniques, such as malware, phishing, social engineering, and hacking, to target banks and steal sensitive information, compromise systems, and execute fraudulent transactions. Bank cybercrime can have severe consequences for the banks and their customers. Financial losses, reputational damage, and legal liabilities are just some of the potential outcomes of bank cybercrime. Banks are entrusted with safeguarding their customers' financial assets, and any failure to do so can erode public trust and confidence in the banking system. To prevent and respond to bank cybercrime, banks must invest in robust cybersecurity infrastructure, implement best practices, and train employees to identify and respond to cyber threats. Banks must also have contingency plans in place to respond quickly and effectively to cyber incidents and minimize the impact of any potential breaches.

Attack Details:

The cyber attack on Cosmos Cooperative Bank involved several techniques, including social engineering, phishing, and remote access tools. The attackers used malware to gain access to the bank's internal systems, specifically its SWIFT payment messaging system. Once inside the bank's systems, the attackers manipulated the SWIFT messages to initiate fraudulent transfers of funds to accounts that they controlled.

The attack was executed in two stages. In the first stage, the attackers gained access to the bank's systems by targeting vulnerable points in the bank's network. They used social engineering tactics, such as phishing emails and remote access tools, to gain entry into the bank's systems. Once inside, they installed malware that enabled them to gain control over the SWIFT messaging system.

In the second stage of the attack, the attackers used the malware to initiate fraudulent payment transfers. They altered the SWIFT messages to divert the funds to accounts

in Hong Kong, Dubai, and other locations. The transfers were made in small amounts to avoid detection, and the attackers were successful in transferring a total of Rs. 94.42 crore ($12.5 million) from the bank's accounts.

Response and Impact:

The attack on Cosmos Cooperative Bank was a significant incident that highlighted the vulnerabilities of the banking sector to cybercrime. The bank's management responded quickly to the attack and worked with the authorities to investigate the incident. The bank also took steps to improve its cybersecurity infrastructure and prevent future attacks.

The impact of the attack was significant for both the bank and its customers. The bank lost Rs. 94.42 crore ($12.5 million) due to the fraudulent transfers. The incident also resulted in a loss of confidence among the bank's customers, who were concerned about the security of their accounts. The bank had to bear the cost of reimbursing its customers for any financial losses they suffered due to the attack, which further added to the financial impact of the incident.

Technical Loopholes:

It has been stated that the bank may have failed to adequately invest in its SOC (Security Operation Center), which should have analyzed the traffic coming in.

An analysis was made that the bank’s fraud detection mechanism was non- existent as there should’ve been red alerts when so many overseas transactions were taking place at such a short span of time.

However, in its statement the bank contended it had adequate IT security in place.

Results/Pending investigation:

The panel of experts appointed by the UN Security Council noted a trend in the Democratic People's Republic of Korea's evasion of the financial sanctions of using cyber-attacks to illegally force the transfer of funds from financial institutions and crypto currency exchanges and also stated that the attack was "motivated" by North Korea.

The Special Investigating Team (SIT) had recovered INR 10.25 Cr that was lost in the heist as was revealed on August 2018.

The Hong Kong based bank 'Hang Seng bank' also returned INR 5.72 Cr in the first installment to Cosmos bank. The police also recovered INR 4 Lakh from genuine Cosmos cardholders, who had visited ATMs when the malware was active and withdrew more money than their account balance.

The cyber-crime cell and the Pune police managed to refund the money to the victims. This action was initiated when the victims who had lost their money had approached the cyber-crime cell.

The cyber cell got in touch with the law enforcement agencies of the 28 countries (including The United Kingdom, United States, United Arab Emirates, Canada and more) for further action.

The Pune Police and the Maharashtra Cyber Cell probing the case are yet to trace the mastermind in the case. As until 19 September 2019, 18 people were arrested by a special investigation team of the Pune Police. The local module busted by the police could be "money mules" — people who serve as intermediaries for criminals and criminal

organizations — acting on behalf of operators abroad.

In a 378-page report by the SIT committee it was stated that “The attack was a more advanced... and highly coordinated operation that bypassed three main layers of defense contained in International Criminal Police Organization (INTERPOL) banking/ ATM attack mitigation guidance”. The report further added “Not only were the actors able to compromise the SWIFT network...to transfer the funds to other accounts, but they simultaneously compromised internal bank processes to bypass transaction verification procedures and order worldwide transfers to almost 30 countries where funds were physically withdrawn by individuals in more than 10.000 separate transactions over a weekend”

Impact on the business of the bank:

The bank was neither penalized for its weak cyber-security nor has anyone been held accountable. This highlights the need for RBI to enforce its cyber guidelines for cooperative banks as strictly as it has for commercial banks. Extensive audit reports had been called for.

The bank's annual report reported total amount involved in the attack to be INR 100. 22 crore, including exchange loss on payment settlement. That was not the only impact. The bank says that “the cyber-attack and restoration of payment systems back to normalcy caused an impact on the customers and their transactions.

Timeline of refund by Pune police:

January 2020 Rs 8.37 lakh

February 2020 Rs 5.98 crore

March 2020 Rs 27.25 lakh

April 2020 Rs 50.52 lakh

Lessons Learned:

The cyber attack on Cosmos Cooperative Bank highlights several lessons for the banking sector. Firstly, it emphasizes the importance of investing in robust cybersecurity infrastructure that can detect and prevent cyber attacks. Secondly, it highlights the importance of employee training and awareness programs to prevent social engineering attacks. Thirdly, it emphasizes the need for banks to have contingency plans in place to respond to cyber attacks quickly and effectively.
The incident also highlights the importance of implementing security measures, such as two-factor authentication, to prevent unauthorized access to the bank's systems. Additionally, banks must conduct regular vulnerability assessments and penetration testing to identify potential weaknesses in their systems and networks.

References:

1.https://www.cyonn.com/post-1/case-study-of-cosmos-bank-cyber-attack
2.https://www.financialexpress.com/industry/banking-finance/how-rs-94-crore-online-fraud-was-carried-out-in-punes-cosmos-bank/1286068/
3.https://www.researchgate.net/publication/357579914_Cyberattack_at_Cosmos_Bank_Regaining_Customer_Trust

Course Outcomes:

1. Identify Threats to Information Security and types of attacks.
2. Understand Information security Risk Management.
3.Detect threats and Prevent attacks to provide security of network.
4. Understand Cyber Crime, Cyber Laws and compliance standards.

Conclusion:

The cyber attack on Cosmos Cooperative Bank was a significant incident that highlighted the vulnerabilities of the banking sector to cybercrime. The incident emphasizes the need for banks to invest in robust cybersecurity infrastructure, employee training and awareness programs, and contingency plans to prevent and respond to cyber attacks. The incident also underscores the importance of implementing security measures, conducting regular vulnerability assessments, and penetration testing to identify potential weaknesses in banking systems and networks. By implementing these measures, banks can better protect themselves and their customers from the financial and reputational damage caused by cyber attacks.