A CASE STUDY ON CYBER SECURITY THREAT TO COSMOS BANK

Dhaarani S. & Aaliya Ameer.A, Tamilnadu Dr. Ambedkar Law University (SOEL)

ABSTRACT

The practice of safeguarding computers, servers, mobile devices, electronic systems, networks, and data from attacks that are malicious is known as cyber security. It is also referred to as information technology security or electronic information security. Risk management, data integrity, security knowledge training, and risk analysis are all components of financial cybersecurity. Data security also includes the protection of sensitive material. Cybersecurity threats are continuously evolving, and the banking industry must take precautions to stay safe. When new defenses threaten more recent attacks, hackers adapt by creating tools and strategies to compromise security. Cyber-security encounters three types of threats they are Cybercrime, cyberattacks, and cyberterrorism. In recent years banking industries rely on online banking, both mobile and web services have weak security systems, making cyber security threats more prevalent. The roll-out of COVID led to the banking sector's digitalization. Both the front-end and back-end processes are now digital. With all of this evolving technology, cyber-attacks are on the rise, and attackers are actively seeking victims for malicious cyber-attacks on banking and financial systems' private data. Generally, cybercriminals prefer to target the banking sector to obtain customer and staff information details, which they then use to steal bank data and money. This research paper in particular aims to study the cyber security threat received by “Cosmos bank” which became the victim of a major cyber malware attack on August,2018. The aim of this research is to study the intense malware attack, the overall effect on the bank due to the attack and to suggest ways to secure cyber security threats to banking industries.

Keywords: cyber-security, cyber-security threats, banking sector, cosmos bank, malware attack

INTRODUCTION

With an increasing number of users, devices, and programmes in the contemporary enterprise, as well as an increased deluge of data, much of which is sensitive or confidential, the significance of cybersecurity is growing. The increasing volume and sophistication of cyber attackers and attack techniques exacerbates the issue.

CYBER SPACE

Along with the rapid development and wide application of information technology, human society has entered the information era. In this era, people live and work in cyberspace. Cyberspace is the collection of all information systems; it is the information environment for human survival.

CYBER SECURITY

The term "cyber security" covers all facets of safeguarding a company's assets, individuals, and operations from cyber risks. A variety of cyber security solutions are needed to reduce business cyber risk as cyberattacks become more frequent and sophisticated and corporate networks become more complicated.

CYBER SECURITY THREATS

The cybersecurity risk in financial sector has transformed the paradigm of banking operations over a number of decades as it has the potential to interrupt banking operations and result in massive direct and indirect losses. The rapid adoption of online services and operations has made banks and other institutions vulnerable to more security threats. The development of cyber technology over the past few decades has altered how the global financial industry operates because most institutions now provide services and carry out business in a virtual setting that is susceptible to security risks like malware, phishing, internal and external system abuse and cyberattacks. Institutions frequently struggle to provide an adequate collection of resources, technologies, training, and best practises to safeguard networks and data from illegal access, which creates cybersecurity risk. As the financial sector globally relies more on cyber technology for its operations and services, banks and financial institutions are more exposed to the systematic risk of technology that cannot be removed. It occurs because a single breach in a banking network could shake off

the entire financial system and bring disastrous aftermath as all banks and financial institutions are interconnected. Financial institutions must have the budgetary resources to procure the essential technology to sustain the cyber infrastructure's resistance to cyber threats.

It is not easy to find the optimal investment in the cyber security infrastructure that can restrain the growth of cybercrimes, as no system is 100% secure from cyberattacks. Breach of cyber security system is unavoidable as some unknown system flaws always exist, regardless of how advanced the technology is. The effects of a cyber-breach and malicious activities may reach far away from the measurable direct financial losses due to direct and indirect costs for the loss of customer's confidence, aftermath of cybercrime, costs associated with the loss of confidential business information and intellectual property, and loss of reputational damage of the hacked institution.

CYBER SECURITY IN INDIA

With initiatives like "Made in India" and "Digital India" having a beneficial impact on the economy overall, India is making quick progress towards its digital goals. Yet, because of its reliance on linked networks and systems, cyber security IS a problem. India is one of the most often attacked nations online, therefore securing vital assets depends on its cyber resiliency.

In the year 2020, CERT- In handled 1,158,208 incidents which included Website Intrusion and Malware, Propagation, Malicious Code, Phishing, Distributed denial of service attacks, website defacements, Unauthorized network Scanning/Probing activities, Ransomware attacks, Data breach and vulnerable services. With continuous efforts at improvement, India has moved up 37 places to be ranked 10th in the Global Cyber security Index 2020(GCI), according to a report by the international telecommunication Union (ITU). In May 2022, CERT -In mandated compulsory reporting of all Cyber-attacks by government and other entities within six hours.

India has implemented a number of statutory and administrative measures to strengthen its cyber defence and successfully combat cybercrime. There are two legislations: the Information Technology Act 2000, provides the legal framework for addressing cybercrimes and cyberattacks.

Criminal countermeasures include the use of this act along with the Indian Penal Code.

COSMOS BANK CASE SUMMARY

In one of the largest cyberattacks on an Indian bank, Several cloned debit cards from Cosmos Bank were used for thousands of ATM withdrawals from India and 28 other countries over the course of seven hours on August 11, 2018. While more than 12,000 ATM withdrawals totaling roughly

Rs 78 crore were made outside of India, another 2,800 transactions totaling Rs 2.5 crore were performed in various locations within India. Also, utilising the SWIFT service, more than Rs 13.92 crore were sent to a Hong Kong-based firm on August 13, 2018. According to an investigation, Visa cards were used for transactions outside of India while RuPay cards were used within of

India. In this case, which was reported to the Chaturshringi police station under sections 120B, 420, 467, 468, 469, 471, and 34 of the Indian Penal Code and the pertinent provisions of the Information Technology Act, a total of Rs.94 crore was embezzled.18 people have been detained by the police thus far in connection with this case. Nine suspects were named in a 1,700-page chargesheet that was submitted in December 2018 by the special investigation team (SIT) looking into the matter. Then, nine additional defendants were named in two extra charge sheets. Pune City Police and Cosmos Bank have succeeded in getting back Rs.5.72 crores that fraudsters transferred into a bank in Hong Kong.

SIGNIFICANCE OF THE STUDY

This study aims at understanding the emerging cyber space and security to the financial sector especially in the banking sector in India. Since the whole of the banking sector is developing with the help of AI (Artificial Intelligence), it is important to protect it against various cyber security threats that it may face. This research study understands the extent of a cyber-attack with the help of the case of "Cosmos bank" malware attack. The severance of the attack and the aftereffects are analyzed under this case study. It also suggests ways to control, protect against and overcome cyber security threats to the banking sector.

REVIEW OF LITERATURE:

1) Kutub Thakur,.et.al., ”An Investigation on Cyber Security Threats and Security Models “,IEEE 2nd International Conference on Cyber Security and Cloud Competing , New York,USA,pp.307-311,doi:10.1109(2015): This paper studies the cyber security models, it's framework along with their limitations and review the past techniques used to mitigate these threats.

2) Diptiben Ghelani,et.al.,”Cyber Security Threats, Vulnerabilities and Security Solutions Models in Banking”, American Journal of Computer Science and Technology, Vol.x,No.x,doi:10.11648(2022): This study proposes that Smart Online Banking Systems (SOBS) be made more secure by employing biometric prints, which decreases the number of threats that an intruder might pose.

3) Md.Hamid Uddin,et.al.,”Cyber Security Hazards and Financial System Vulnerability: A Synthesis of literature”, Risk Manag 22, 239-309,doi:10.1057(2020): This paper provides a systematic review of the growing body of literature exploring the issues related to pervasive effects of cyber security risk on the financial system.it also proposes five new research avenues for consideration.

4) Derek Mohammed, “Cyber Security Compliance in the Financial Sector”, Journal of Internet Banking and Commerce,ISSN: 1204-5357,1st April(2015): This paper contrasts the values nad the issues created by increasing compliance requirements for the financial sector. It also reviews the similarities and difference among compliance environments created by financial regulations.

5) H.M.Alzoubi,et.al., “Cyber Security Threats on Digital Banking”,2022 International Conference on AI in Cyber Security(ICAIC),TX,USA,pp.1-4,doi:10.1109(2022): This paper focuses on an efficient security system that involves multiple verifications, authentication processes and data encryption are needed to combat cyber security threats.

STATEMENT OF PROBLEM:

When it comes to digital banking privacy and protection of the customers data becomes a

top priority. But with the emergence of cyber space though it comes with benefits, it has become difficult to protect customer data with the uprising of cyber security threats and attacks. These cyber-attacks are becoming more prevalent in the financial sector. Hence it is important to resolve this problem by putting up a strong shield to protect from cyber security threats. This is essential since in the present world all these data are kept and maintains in a digital form. This study suggests ways to protect against cyber security threats and consequences.

OBJECTIVES OF THE STUDY

The objectives of the study are:

1) To find out the intensity of the cyber attack on Cosmos bank.

2) To find out the consequences and overall effect on the bank due to the malware attack.

3) To suggest ways to protect digital banking and the financial sector from cyber security threats.

LIMITATIONS OF THE STUDY

- This study is limited to the cyber security threats only in the financial sector.

- This study uses secondary data that is annual reports collected from the website of the Cosmos bank.

- This study is not limited to any person, profession, educational qualification, income, wealth, race and geographical area.

METHODOLOGY

Methodology explains the research path to be taken, the tools to be used, the scope and sample of the study for data collection, the tools for data analysis used, and the pattern of establishing conclusions. For this study we used secondary data. The data which is required for this study has been collected from the annual bank reports from the website of the

Cosmos bank. The annual reports have been collected for 5 years starting from the year 2018 – 2022.

TABLE 1: COSMOS BANK ANNUAL REPORT 2018 – 2019

(₹ in crore)

PARTICULARS	2017-2018	2018-2019
Share Capital	371.64	344.47
Reserves	1,612.45	1,515.86
Own Funds	1,984.09	1,860.33
Net NPA	7.24%	6.30%
Gross NPA	9.45%	8.53%
Total Income	**1,876.94**	**1,820.63**
Total Income (After transferring funds from Reserves)	**1,949.36**	**1,874.34**
A) Interest Received	1,461.68	1,462.75
B) Other Income	204.54	203.23
C) Other Credits	210.72	154.65
D) Transferred from Reserves	72.42	53.71
Total Expenditure	**1,942.67**	**1,798.80**
A) Interest Paid	1,099.56	1,051.03
B) Establishment Expenditure	157.99	176.36
C) Other Expenditure	184.95	242.07
D) Provisions + Write Off	500.17	329.34
Net Profit / Loss	**-65.73**	**21.83**
Net Surplus	**6.69**	**75.54**

Source: 113th Annual Report of Cosmos Bank, pp: 21

INTERPRETATION:

This was the annual report of the year of attack . As we can see that the share capital in 2018 – 2019 has reduced by 27.17 crores than the year 2017 –2018. The Net NPA has reduced by 0.067%. The gross NPA has reduced by 0.086 %. The total income has reduced by 56.31 crores. The total expenditure has reduced by 143.39 crores. Hence in this year there is a profit of 21.83 crores. Also, the total income after transferring funds from the reserve has decreased by 75.02 crores.

TABLE 2: COSMOS BANK ANNUAL REPORT 2019 – 2020

(₹ in Crores)

PARTICULARS	2018-2019	2019-2020
Share Capital	344.47	322.67
Reserves	1,515.86	1,651.41
Own Funds	1,860.33	1,974.08
Net NPA	6.30%	7.15%
Gross NPA	8.53%	9.41%
Total Income	**1,874.34**	**2,085.92**
A) Interest Received	1,462.75	1,442.00
B) Other Income	203.23	326.02
C) Other Credits	208.36	317.90
Total Expenditure	**1,798.80**	**2,121.75**
A) Interest Paid	1,051.03	1,073.14
B) Establishment Expenditure	176.36	203.89
C) Other Expenditure	242.07	235.73
D) Provisions + Write Off	329.34	608.99
Net Profit / Loss	**21.83**	**-54.34**
Net Surplus / Short-fall.	**75.54**	**-35.84**

Source: 114th Annual Report of Cosmos Bank, pp:33

INTERPRETATION:

As we can see here the share capital in 2019– 2020 has reduced by 21.8crores than the year 2018 –2019. The Net NPA has increased by 0.67%. The gross NPA has increased by 0.86 %. The total income has increased by 211.58 crores. The total expenditure has increased by 322.95 crores. In this year there is a short fall of 35.84cores. Hence it is a loss for the bank.

TABLE 3: COSMOS BANK ANNUAL REPORT 2020-2021

(Amt in Crore)

Particulars	2019-20	2020-21
Share Capital	322.67	333.59
Reserves	1,651.41	1,738.70
Own Funds	1,974.08	2,072.29
Net NPA	7.15%	8.75%
Gross NPA	9.41%	11.00%
Total Income	**2,085.92**	**2,081.23**
a) Interest Received	1,442.00	1,360.75
b) Other Income	326.02	463.18
c) Other Credits	317.90	257.30
Total Expenditure	**2,121.75**	**2,024.45**
a) Interest Paid	1,073.14	977.56
b) Establishment Expenditure	203.89	201.65
c) Other Expenditure	235.73	183.37
d) Provisions + Write Off	608.99	661.87
Net Profit/ Loss	**-54.34**	**56.78**
Net Surplus/Shortfall	**-35.84**	**56.78**

Source: 115th Annual Report of Cosmos Bank, pp: 29

INTERPRETATION:

In this annual report the share capital in 2020 – 2021 has increased by 10.92 crores than the year 2019 –2020. The Net NPA has increased by 0.81 %. The gross NPA has increased by 0.996 %. The total income has reduced by 4.69 crores. The total expenditure has reduced by 97.3 crores.

Here the bank has profited by 56.78 crores.

TABLE 4: COSMOS BANK ANNUAL REPORT 2021 – 2022

(Amt in Crore)

Particulars	**2020-21**	**2021-22**
Share Capital	333.59	335.34
Reserves	1738.70	1765.27
Own funds	2072.29	2100.61
Net NPA	8.75%	4.74%
Gross NPA	11.00%	6.86%
Total Income	**2081.23**	**1908.53**
a. Interest Received	1360.75	1397.96
b. Other income	463.18	191.35
c. Other Credits	257.30	319.21
Total Expenditure	**2024.45**	**1842.62**
a. Interest Paid	977.56	805.41
b. Establishment Expenditure	201.65	208.32
c. Other expenditure	183.37	205.77
d. Provisions + write off	661.87	623.12
Net Profit / Loss	**56.78**	**65.91**
Net surplus / shortfall	**56.78**	**77.91**

Source: 116th Annual Report of Cosmos Bank, pp: 29

INTERPRETATION:

In this annual report the share capital in 2021– 2022 has increased by 1.75crores than the year 2020 –2021 The Net NPA has reduced by 0.83%. The gross NPA has reduced by 0.102 %. The total income has reduced by 172.7crores. The total expenditure has reduced by 181.83crores. In this annual report it shows that the bank has a short fall of 77.91 crores.

RESULTS AND DISCUSSIONS:

It is understood from the above table that the bank has suffered a huge loos during the year of 2018 – 2019, which was the year of the attack. The bank has regained some profits and some losses in the upcoming years that is from 2019 – 2022. During the year of 2018 – 2019 the resulting financial loss was enormous. The cyber attack disrupted Cosmos Bank's digital banking services, damaging its reputation and significantly reducing customer trust. As a result of the event, the entire banking sector, especially the cooperative, was shocked. The total damage from the attack is 94 million rupees, or $13.5 million. Cosmos Bank had to shut down its ATM operations and suspend online and mobile banking services. The attackers acted in the cyber attack on the 29th countries and more than 12,000 transactions worth 81.99 crowns were made through ATMs using VISA debit cards and 2,800 transactions with a value of 2.75 million from domestic ATMs Rupay cards. After the attack the bank brought up new policies and protection methods to protect against hackers and cyber security threats. It is also observed that the total income and expenditure for the year 2018 –2019 was receding, while for the year 2019 –2020 it was increasing, again it receded during the years 2020-2021 and 2021-2022. Hence it is observed that the bank had and an increase in their total income and expenditure only during the year 2019 – 2020 while it has receded

SUGGESTIONS

The world of cyber security is constantly changing and threats and constantly evolving. In the banking and financial sector, the stakes are high, not only are large sums of money at risk, but if banks and other financial systems are compromised, the disruption to the entire economy can be significant. Whether it’s a digital – only bank or a bank with a branch, the challenges are similar, but as our world moves to the digital frontier, banks that want to meet demand without compromising security must overcome some key cybersecurity challenges. With so many cyber threats to contend with, even a prudent financial institution would do well to proactively protect against them. Some of the ways to overcome against these threats are to address the talent gap by collaborating with other organizations and security partners that provide managed services for protection. By implement ongoing security awareness training programs or evaluate existing programs to ensure they are relevant and up-to-date with the current threat environment. Buying detection and response tools to help you be

proactive and prevent attacks. Implement consumer awareness programs to prevent customers from disclosing sensitive details to cybercriminals. Communication is very important in banks and other financial institutions if they want to increase awareness of cyber security in banking and prevent financial cyber security incidents. Design appropriate internal communication strategies to keep employees informed of their responsibilities to keep data secure, report breaches and be aware of emerging threats, and ensure you have the appropriate tools and resources to communicate information in an engaging and engaging way. Some banks can achieve this through internal financial communications, including, using company wallpapers and screensavers to remind employees about security issues. Conduct security training for employees and regularly test their knowledge of banking cyber security. Provide information about new threats so employees can be alert. Regularly post tips and tricks on cybersecurity best practices don't overload yourself with too much information at once. Use different communication channels to reinforce your messages. In these ways cyber security threats can be reduced in the banking sector.

CONCLUSION

Every organization is concerned about cyber security. It is very important that banks have adequate cyber security solutions and procedures, especially for institutions that hold a lot of personal data and transaction lists. Cyber security in banking is an undisputed topic. Hackers are more likely to target the banking sector as digitization progresses. The main goal of banking cyber security is the security of the user's assets. When people run out of money, further actions or transactions are done online. Individuals use digital money, such as debit and credit cards, to make transactions that need to be protected by cyber security. Today, the assessment that a major cyberattack threatens financial stability is axiomatic—it's not a matter of if, but when. But governments and companies around the world continue to struggle to contain the threat, as it remains unclear who is responsible for protecting the system. Hence it is important to safeguard the data of the customers with efficient cyber security systems and software. This study has given an in-depth analysis on the Cosmos malware attack and the study has also given ways to overcome these cyber security threats to financial and banking sector.

REFERENCES JOURNALS:

Kutub Thakur,.et.al., "An Investigation on Cyber Security Threats and Security Models", IEEE

2nd International Conference on Cyber Security and Cloud Competing , New York,USA,pp.307311,doi:10.1109(2015)

2)Diptiben Ghelani,et.al.,"Cyber Security Threats, Vulnerabilities and Security Solutions Models in Banking", American Journal of Computer Science and Technology,

Vol.x,No.x,doi:10.11648(2022)

Md.Hamid Uddin,et.al.,"Cyber Security Hazards and Financial System Vulnerability: A Synthesis of literature", Risk Manag 22, 239-309,doi:10.1057(2020)

Derek Mohammed, "Cyber Security Compliance in the Financial Sector", Journal of Internet Banking and Commerce,ISSN: 1204-5357,1st April(2015)

H.M.Alzoubi,et.al., "Cyber Security Threats on Digital Banking",2022 International Conference on AI in Cyber Security(ICAIC),TX,USA,pp.1-4,doi:10.1109(2022)

WEBSITES:

1) https://indianexpress.com/article/cities/pune/pune-cosmos-bank-cyber-attacksupplementary-chargesheet-filed-against-five-from-thane-6120232/

2) https://www.tatacommunications.com/blog/2018/09/lessons-learnt-from-cosmos-bankattack/

3) https://www.studocu.com/in/document/manipal-academy-of-higher-education/cybersecurity/cyber-attack-news/24353558

4) https://www.authorea.com/doi/full/10.22541/au.166385206.63311335

5) https://ieeexplore.ieee.org/abstract/document/7371499/references#references

6) https://www.gov.je/StayingSafe/BeSafeOnline/ProtectYourBusinessOnline/pages/10steps tocybersecurity.aspx

7) https://www.theglobaltreasurer.com/2019/09/25/the-importance-of-cyber-security-inbanking/

8) https://www.guardrails.io/blog/the-top-ten-cyber-security-threats-to-digital-banking-andhow-to-guard-against-them/

9) https://intellipaat.com/blog/cyber-security-in-banking/#26

10) https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financialsystems-maurer.htm