International Journal of Innovations & Research Analysis (IJIRA)
ISSN : 2583-0295, Impact Factor: 5.449, Volume 02, No. 02, April - June, 2022, pp 19-23

CYBER-ATTACKS ON BANKING INSTITUTIONS IN INDIA: SAFETY AND PREVENTIVE MEASURES

Dr. Narendra Kumar Batra*
Ms. Parul Gulati**

ABSTRACT

The goal of this research paper is to look at the devastating effects of cybercrime on banking institutions, as well as the cyber security methods that have been tried to mitigate its impact and the construction of a solid cyber security framework. Banks have been the primary victims in recent years. In India, a number of institutions are frequently targeted by large-scale malware assaults, which not only expose important and sensitive data but also result in significant financial losses. The aim of this paper is to determine which company areas are more vulnerable to cyber-attacks and to ensure that cyber security protocols are customized and developed. The research comprises secondary data analysis from a variety of digital resources, including government websites, journals, and research papers, as well as case study analysis of various cyber dangers and crimes that have resulted in significant financial loss in the past. This paper will present information about the cyber regime that will assist banks, financial institutions, and society as a whole.

Keywords: *Cyber Security, Cyber Crime, Sensitive Data, Cyber Attacks.*

Introduction

The banking and financial services industry (BFSI) is a massive industry with millions of consumers all over the world. Banking services have been made more accessible to the impoverished and disadvantaged elements of society. Over time, this number has risen. According to research, the majority of Indians are adopting a digital approach, with 51 percent preferring online banking channels and 26 percent using bank websites and mobile banking services. With the rapid expansion of bank digitization, cyber dangers have arisen as a major source of concern. According to Gulshan Rai, the banking industry accounted for only 22% of the cyber-attacks that occurred in India.

Over the last decade, there has been a massive growth in cyber invasions and attacks. This enormous rise in crime has not just wreaked havoc on the financial system. Cybercrime costs the global economy roughly USD 114 billion per year, while the cost of combatting the crime is USD 274 billion. In India, the evolution of cyber threats began in 1998 after the banking industry was privatized, with virus attacks, followed by hacking websites, sending malicious codes, advanced worm and Trojan, identity theft (Phishing), Denial of Service (DOS), and Distributed Denial of Service (DDOS) in subsequent years, and now with cyber espionage and cyber warfare. Some of the previous cyber-attacks on Indian banking industry include a $171 million phishing email attack on Union Bank of India in July 2016, a May 2017 ransomware attack that locked down thousands of machines, and so on.

* Head, Department of Commerce, Ram Lubhai Sahni Government Mahila Mahavidyalaya, Pilibhit, U.P., India.
** Research Scholar, MJP Rohilkhand University, Bareilly, U.P., India.

The inherent vulnerabilities in bank systems and software, the numerous entrance points to the internet, and obsolete defence technologies that are particularly vulnerable to advanced assault technologies utilised by hackers are all cyber security concerns. The most basic goal of banking institutions, however, is mandated cyber security readiness. A variety of regulatory processes and cyber security technologies have been developed in recent years as a result of the growing dangers to the cyber infrastructure in its regulated businesses. As a result, given the growing frequency and complexity of cyber security incidents, a constant analysis of the cyber security landscape and emerging threats is required. The progress of banks in increasing their cyber security resilience and responsiveness will be tracke

Study's Goal: As a result, the goal of this research is to examine the threats that exist in the industry. The goal of this article is to examine the threats that exist in present and developing technologies, as well as the processes that may be used to conduct a continuing analysis of the cyber security landscape and emerging threats.

- Examine the impact of cybercrime on the financial industry.
- Plans to research innovative technologies in order to meet the problems posed by cyber threats.
- Suggest the implementation of various security protocols/standards, as well as necessary policy intervention, by interacting with stakeholders.

Review of the Literature

The introduction of a new era in banking technology that has resulted in an increase in cyber-crime by removing the necessity for physical presence at the bank for many transactions and other financial services by using electronic devices. Because of the rising reliance of consumers on the internet for everything from small monetary transactions to massive financial affairs, e-banking has made a significant and outstanding contribution to this upswing. According to a report, losses due to e-banking fraud increased by 48 percent in 2014 when compared to 2013 . In India, the growth of the cyber world, combined with customers' increasing needs for convenience access from different devices for transaction purposes, plays an inexorable role.

According to studies, India accounts for 7% of all cyber fraud incidents worldwide. Indian banks have been targeted by possible state and non-state actors, organised criminals, and hacktivists on a regular basis. The cyber-attack on Canara Bank in 2016 exemplifies this better, with a hacker from Pakistan attempting to disrupt the bank's e-payments by vandalising its website and inserting dangerous software . In July 2017, an attack on Union Bank of India's Nostro account resulted in the loss of over USD 170 million. According to sources, the criminals used spear phishing to acquire access. It was pre-supposed in a 2017 poll on cybercrime performed by KPMG. According to a Deloitte report on cyber-crime released in 2015, 93 percent of respondents said there has been an increase in fraud cases in the banking industry in the last two years, with less than 25 percent of fraud losses recoverable due to the long time lag between cyber-attacks and detection of the threat and attackers. Despite global fraud warnings, a huge number of Indian banks did not place enough attention on fraud and risk management solutions. Unfortunately, just 20% of all banks considered Fraud Risk Management to be an effective means of fraud control, and a considerable majority of these banks only learned this after they were hacked. The devastating impact of cybercrime on banking institutions' performance, as well as the strenuous efforts made to protect the banking industry from cyber-attacks and growing competition among banks, have prompted researchers, policymakers, and cyber experts to identify and analyse cyber-crime zones, cyber criminals' intentions, and vulnerable points susceptible to cyber-attack.

The study's main goal is to create a world-class cyber security framework that will avoid loss while also facilitating growth and output. Despite the fact that numerous research have been conducted on cyber-crime on banking platforms, there is still much dispute and misinformation. Some claim that too much digitization has resulted in the creation of cyber-crime platforms and advocate for a defensive safety protocol. Others that support digitization as a modern technology emphasise the importance of having a world-class consistent cyber security system in place to suit digitization's needs. A large body of literature has accumulated in this topic as a result of the lack of consensus. However, there has been little progress in eliminating or reducing cyber-crime in financial organisations, particularly banks. Rather, there are study gaps which are widening.

In this context, this study is an attempt to supplement the existing literature and fill a research gap by looking into critical loopholes in the banking process that are frequently overlooked by bankers, as well as looking into developing a common platform to take a frontal attack on cyber-crime and the associated attitudinal poverty

Research Methodologies

To conduct this research, existing information/data from multiple sources is gathered and examined on a comparative basis in order to arrive at logical conclusions/answers to the research topic. White papers, government documents, published academic papers, journals, print media, RBI, NCRB, NITI Aayog, and CERT-IN findings, statistical data bank, and historical records are the most common sources.

Because a good collection of data already exists in a documented form, a secondary method of data gathering and analysis is used in this scenario. Given the subject matter and time constraints, conducting a direct study may not be a viable option. Finding reports of previous cyber-crime scenarios and listing of preventive measures to provide an anti-cybercrime platform is done from a historical perspective. Through a case study methodology, more measures have been made to examine the impact of cyber-attacks. The research's goal is to define the points in the banking process that are more vulnerable to attack and identify the types of cyber-attacks that banks are likely to face on a daily basis, narrowing the focus to bank fraud cases in India.

Cyber Threats have Evolved

In the 1980s, a basic computer virus kicked off the evolution of cyber-attacks. Viruses are self-replicating computer programmes that change other programmes and insert their own code in order to infect the system. With some applied research in the late 1990s, hacking websites evolved as a danger to systems. Malicious code as an attack emerged in 2004, posing a threat to application security that could not be managed by traditional antivirus alone. Attack scripts, viruses, Trojan horses, worms, and harmful material are all examples of these codes, which represent a broad range of system security terminology. Then, as attacks became more sophisticated, complex Trojans and worms returned. In late 2008 and early 2012, attacks such as identity theft and phishing were common. Then, in late 2015, attackers evolved with significant threats including DOS and DDOS attacks, and after that year, cyber espionage and cyber warfare became widely used as a type of attack, till now. DDOS attacks are more pervasive and dangerous than DOS attacks because they utilise many internet connections, and victims are unable to identify the source of the attack [7].

- **Phishing**

Phishing attacks are designed to collect user information such as usernames, passwords, credit card numbers, and PINs in order to get access to the victim's bank account or seize control of social media data.

- **Identity Theft**

A type of cybercrime in which hackers attempt to access crucial personal data such as social security numbers, Aadhar numbers, credit card numbers, and other associated information in order to mimic someone and profit off their identity.

A high rate These are turned on when you open scam email attachments [8].

For the goal of ransom, a phone was used to acquire access to private personal data from the general public.

Viruses and Trojans (section 4.1.3)

Viruses are nothing more than malicious instructions that multiply themselves in the same way that human viruses do without the assistance of humans. The Trojan virus is a disruptive programme that, unlike viruses, does not replicate itself but spreads quickly. These are turned on when you open scam email attachments [8].

- **Fishing**

This is the use of social engineering over the phone to get access to private personal data from the general public in order to extract a ransom.

Cross-site scripting (CSS) is a type of scripting that is commonly utilised in web applications. This allows attackers to insert client-side scripts into user-facing web pages. Assailants utilise this to get around access constraints.

- **Insider Threat**

This is a hostile threat that originates from within a company, from personnel, and exposes the system to attackers.

- **Botnet**

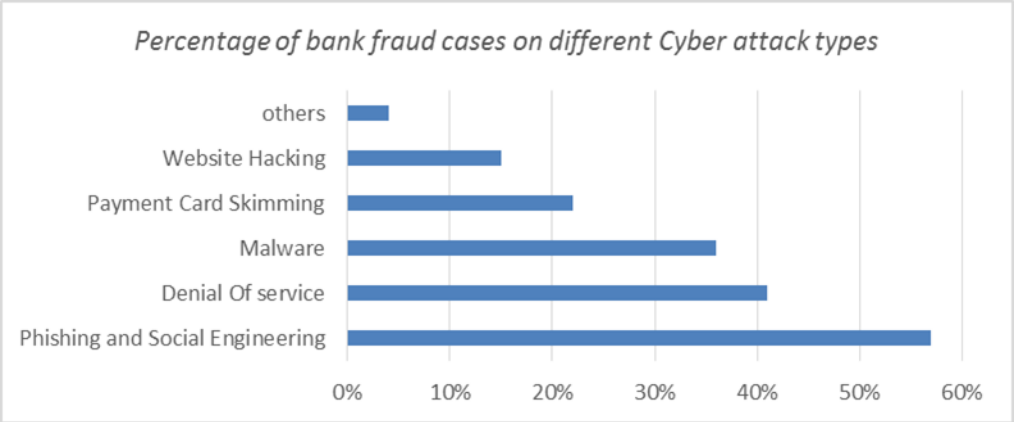
A botnet is a sort of cyber-attack in which malicious code infects a network of private computers, which are then controlled by a group without the owners' knowledge [8].

- **ATM/Debit/Credit Card Frauds**

In these types of frauds, the fraudster attaches a skimming device to the ATM or POS machine's keypad so that it is not visible to the naked eye. When a customer inputs his card number and PIN, the information is sent to a skimmer that has been placed and can be used to steal money.

- **Ransomware**

Ransomware is one of the most well-known cyber-threats. This is a sort of malicious software that prevents a computer or a group of computers from accessing the internet unless a certain amount of money is paid. They threaten to reveal critical information unless the attackers are given a certain amount of money. A typical sort of ransomware assault is Maze.



Statistics And Analysis

So, why are financial institutions so vulnerable to cyber-attacks? The most common reason for attacks appears to be money, which drives attackers to do anything. Aside from that, the Indian financial sector has a massive market that is developing by the day. To this day Huge numbers of online and offline users are now transacting through various modalities such as net banking, mobile banking, mobile wallets, credit/debit cards, and so on, thanks to the spread of digital banking systems and financial inclusion programmes in India. According to RBI data, bank deposits expanded at a CAGR of 11.11 percent from FY09 to FY17, totaling $1.86 trillion USD by FY19. As of February 2020, deposits totaled $1893.77 billion [9]. Table 1 shows statistics data on the number of transactions.

Table 1: Transactions and Value of Transactions through Various Modes as ofMay 2020

Mode	No of transactions (in lakhs)	Amount (in Lakhs)
NEFT	1929.4	148174950
RTGS	9003796	704186936
Credit card	77492598	2101749
Debit Card	507963710	15853983
Mobile wallet	3958.3	1585800

(Source: RBI Bulletin 2020 All Values in Lakhs)

Findings and Results

Phishing, identity theft, and malware are the most common crimes in the Indian banking sector.

Small mistakes and a lack of information about cyber security policies can lead to major crimes. Any suspicious activity should be treated with caution, and concerned authorities should be notified first before taking action.

- Systems should be audited at regular intervals to check for security breaches.
- Public sector banks should devote more resources to improving security through public-private partnerships; additional funds should be allocated to data protection and security framework enhancement.
- ATM/POS machine switching system connectivity with core banking system, as well as ATM/POS machine transaction monitoring, should be regularly monitored. To verify connectivity, a consistent network packet as an acknowledgement signal should be delivered and received.

Mechanism of Protection

Cyber-attacks are evolving in tandem with the advancement of technology. To obtain privilege and disrupt the network, attackers have gotten more competent at researching and accumulating weaknesses and locating flaws in the system. Banks are now adopting the latest cyber-security technologies and are willing to invest more budget to safeguard their environment from unauthorised access and unwanted data and security breaches in order to become well informed and progressed with the latest hacking modus operandi. The banking sector can be protected from unauthorised attacks by properly configuring and maintaining the firewall.

Banks should implement a variety of security measures to protect themselves against known cyber-attacks. There are several ways to test the security of a bank's network and infra to test the security of a bank's network and infrastructure.

References

1. L. Klapper, D. Singer, S. Ansar, and J. Hess, “Asli Demirgüç-Kunt The Global Findex Database Measuring Financial Inclusion and the Fintech Revolution 2017.” 2017, [Online]. Available: http://hdl.handle.net/10986/29510.
2. B. Standard, “Banks most vulnerable to cyber threats_ Govt official _ BusinessStandard News.” Business Standard Ltd, Mumbai, pp. 2–10, 2019, [Online]. Available: https://www.business-standard.com/article/current- affairs/banks-most-vulnerable-to-cyber-threats-govt-official-119022000646_1.html.
3. R. Raghavana and L. Parthiban, “The effect of cybercrime on a Bank’s finances,” Int. J. Curr. Res. Acad. Rev., vol. 2, no. 2, pp. 173–178, 2014, [Online]. Available: http://www.ijcrar.com/vol-2-2/A.R.Raghavan and Latha Parthiban.pdf.
4. K. Mohapatra, “effective operational risk management Cybersecurity vulnerability in Indian banks,” CYBERSECURITY Framew. BANKS, 2016, [Online].Available: https://financialit.net/sites/default/files/customerxps_white_paper_cyber security_vulnerability_in_indian_banks_1.pdf.
5. M. M. MANISHA, J. M. P, and N. K.M, “International Journal of Advanced Research in Online Banking and Cyber Attacks : The Current Scenario,” Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 5, no. 12, pp. 743–749,2015,[Online]. Available: https://www.researchgate.net/ publication/290325373_Online_Banking_and_Cyber_Attacks_The_Current_Scenario.

A. Saravade, N; Bhalla, “Emerging trends and challenges in cyber security _ Reserve Bank Information Technology Private Limited (ReBIT).” 2018, [Online]. Available: https://rebit.org.in/whitepaper/emerging- trends-and-challenges-cyber-security.

6. D. V. Saraswat, “Cyber security,” 2003. doi: 10.1016/j.techsoc.2003.09.022.
7. S. Goel, “Cyber-Crime: a Growing Threat To Indian Banking Sector,” 3rd Int. Conf. Recent Innov. Sci. Technol. Manag. Environ., vol. 2016, pp. 13– 20, 2016,[Online].Available: http://data.conferenceworld.in/IFUNA18DEC16/P13-20.pdf.
8. RBI, “the Reserve Bank ’S Accounts,” 2019. [Online]. Available: https://m.rbi.org.in/ Scripts/AnnualReportPublications.aspx?Id=1267.

❑❍❑