OPEN ACCESS

Volume: 11

Special Issue: 1

Month: March

Year: 2024

E-ISSN: 2581-9402

Received: 03.02.2024

Accepted: 11.03.2024

Published: 22.03.2024

Citation:
Mundhra, Adarsh. "Impact of Cyber-Attacks on Banking Institutions in India: A Study of Safety Mechanisms and Preventive Measures." *Shanlax International Journal of Management,* vol. 11, no. S1, 2024, pp. 142–48.

DOI:
https://doi.org/10.34293/management.v11iS1-Mar.8070

Impact of Cyber-Attacks on Banking Institutions in India: A Study of Safety Mechanisms and Preventive Measures

Adarsh Mundhra
II MBA, School of Management
Dwaraka Doss Govardhan Doss Vaishnav College, Chennai, TamilNadu

Abstract

This study intends to investigate the disastrous effects of cybercrime on financial institutions, as well as the creation of a strong cybersecurity mechanism and attempts to mitigate its effects. Banks are its direct target as of late. Many banks in India are frequently the target of widespread malware attacks, which not only expose private and sensitive data but also result in significant financial losses. This study's goals are to determine which company sectors are more vulnerable to cyberattacks and to guarantee that cyber security protocols are developed and customized. The report includes case study examination of numerous cyberthreats and crimes that have previously resulted in significant financial loss, as well as secondary data analysis from a variety of online resources, including government websites, journals, and research papers. This essay will offer cyber regime insights that will be advantageous to financial institutions, banks, and society at general.

Introduction

The banking and financial sector institution (BFSI) is a massive industry with a vast client base dispersed throughout the world. Over time, there has been an increase in the availability of financial services for the most marginalized and susceptible segments of society. Approximately 1.2 billion people who have opened bank accounts since 2011 are listed in the Global Findex database. According to a survey, the majority of Indians are adopting a more digital mindset, with 51% of them using online banking channels and 26% using mobile banking and bank websites to access services. The remarkable surge in digitization within banks has led to a significant increase in awareness regarding cyber dangers. According to Gulshan Rai , just 22% of cyberattacks that occurred in India were directed on the banking industry. Over the past ten years, there has been a massive rise in cyberattacks and invasions. In addition to severely harming vital banking procedures, this unheard-of rise in criminality has cost the system enormous sums of money.

Cybercrimes cost the world over USD 114 billion in lost revenue annually, while their prosecution costs USD 274 billion . Cyber threats evolved in India primarily in the years following the banking industry's privatization in 1998. These included virus attacks, website hacking, malicious code transmission, advanced worms and Trojan horses, identity theft (Phishing), Denial of Service (DOS) and

Distributed Denial of Service (DDOS) attacks in the years that followed, and cyber espionage and cyberwarfare today. Some of the previous cyberattacks on the Indian banking sector include the ransomware attack that occurred in May 2017 that locked down thousands of machines and the phishing email attack that occurred on Union Bank of India in July 2016 that stole $171 million. India had 42 million cyber-crime victims, 52% of whom suffered financial or some other kind of loss due to hacking, scams, frauds and thefts

Major Cyber security challenges are inherent vulnerabilities in the system and software used by banks, innumerable entry points to internet, and outdated defense technologies that are highly vulnerable to advanced attack technologies used by hackers. However, mandatory cyber security preparedness is the most basic objective of banking institutions. Conscious of rising threats of the cyber infrastructure in its regulated entities, a good number of regulatory mechanisms and cyber security technologies have been evolved during these years. Therefore, recognizing the increased frequency and complexity of cyber security incidences, there is a need to conduct an ongoing review of cyber security landscape and emerging threats. Bankers' progress in strengthening cyber security resilience and response is to be monitored

Objective of the Study

Therefore, the purpose of this article is to examine the risks associated with both new and current technologies, looking at the implementation of measures to

- Continue to monitor the state of cyber security and new threats.
- Examine how cybercrimes affect the banking industry.
- Plans to research cutting-edge solutions to address the difficulties brought on by cyberthreats.
- Recommend adopting different security standards and protocols, interacting with stakeholders and proposing relevant policy interventions.

Literature Review

Cybercrimes have increased as a result of the advent of a new era in banking technology that has made it unnecessary to physically visit the bank for many transactions and other banking services by using electronic devices. The rise of e-banking can be attributed in large part to consumers' greater reliance on the internet for everything from small-scale financial transactions to complex financial matters. According to a report, losses from e-banking fraud increased by 48% in 2014 compared to 2013. The increasing expansion of the digital realm coupled with the rising needs of Indian consumers for convenient access across various platforms for transactional purposes inevitably draws cybercriminals online banking malware. India is ranked third on the list of nations most afflicted by online banking malware, behind the US and Japan, according to a 2014 survey.

It has been reported that 7% of all cyber fraud incidents globally take place in India. Hacktivists, organized crime, and potentially state actors have been targeting Indian banks on a regular basis. This is better explained by the 2016 Canara Bank cyberattack, in which a Pakistani hacker attempted to disrupt the bank's electronic payments by infiltrating its website and inserting malicious software. In July 2017, Union Bank of India was similarly targeted by an attack that resulted in the theft of over USD 170 million from its Nostro account. According to reports, the attackers gained access by spear phishing victims.

It has been assumed in a 2017 KPMG poll on cybercrime that banks were initially vulnerable to widespread cyber threats since they lacked sufficient cyber security measures. Cases of cybercrimes rose from 89% to 94%, while the resulting financial losses rose from 45% to 63%. It also showed that almost 70% of respondents thought their organization lacked the tools necessary to combat cybercrime.

In a 2015 report on cybercrime, Deloitte found that 93% of respondents indicated that the number of fraud cases in the banking sector had increased over the previous two years, and that less than 25% of the fraud losses could be recovered due to the significant lag time between cyberattacks and the identification of the threat and the attackers. A significant portion of Indian banks failed to place enough attention on fraud and risk management solutions, in spite of warnings from fraud instances throughout the world. Regretfully, only 20% of banks considered fraud risk management to be an effective means of controlling fraud, and many of these banks didn't even understand this until after they inadvertently fell prey to cyberattacks. Researcher, policy makers, and cyber experts are focusing on identifying and analyzing the cyber-crime zones, intentions of cybercriminals, and vulnerable points susceptible to cyberattack due to the catastrophic impact that cybercrime has on the performance of banking institutions, the strict measures taken to protect the banking industry from cyberattacks, and the growing competition among banks.

Types of Cyber Attacks

It is clear from the vast array of data gathered from several sources and the analysis performed on that data that these specific cybercrimes mostly impact Indian banking systems. The Verizon 2017 data breach investigation report states that after surveying a number of banking institutions, it was discovered that over 50% of them appeared to have been impacted by the top five cyberthreats, which include ransomware, malware, spear phishing, denial of service (DOS), and phishing. The top three cyberattack patterns, which include denial of service (DOS), online application attacks, and credit card skimmer, account for more than 88% of all security events among the majority of occurrences that are reported.

Phishing

Phishing attempts aim to obtain user passwords, credit card numbers, and PINs in order to gain access to the victim's bank account or take over social network data.

Identity Theft

Phishing attempts seek to steal credit card information, PINs, and user passwords in order to take over social network data or access the victim's bank account.

Virus and Trojans

Viruses are nothing more than the cost of malevolent algorithms that can proliferate without human assistance, much like human viruses. A Trojan virus is a malicious program that, in contrast to other viruses, spreads quickly instead of replicating itself. By opening the attachments in spam emails, you can activate these.

Insider Threat

It is a malevolent danger that arises from individuals, or workers within an organization, leaving the system vulnerable to hackers.

Botnet

This kind of cyberattack occurs when a network of personal computers is compromised with malicious software, allowing a gang to take control of those machines without the owners' knowledge.

ATM/Debit/Credit Card Frauds

In these types of frauds, the perpetrator usually utilizes a skimming device that is hidden from view and attached to the keypad of an ATM or POS system. When a customer inputs his card number and PIN, information is sent to an embedded skimmer that might be used to steal money.

DOS and DDOS

Attacks known as denial of service (DOS) cause the network or services to go offline, preventing affected users from accessing the services. This is achieved by delivering an excessive volume of data, which spams users' network traffic and prevents authorized users from accessing the information. Large profit organizations are the target of DDOS attacks. Even though this kind of assault doesn't result in the loss or theft of important data, mitigating the damage takes a lot of money and time.

Ransom Ware

It is among the most well-known online dangers. This kind of malicious software is intended to prevent access to a computer or collection of computers unless a certain amount of money is paid. They threaten to reveal private information until the attackers receive payment. One typical kind of ransomware attack is maze.

Percentage of Bank Fraud Cases on Different Cyber Attack Types

Statistics and Analysis

Therefore, why are banks so susceptible to cyberattacks? Money appears to be a major factor in attacks, making assailants blind and unable to take any action. In addition, the Indian financial sector has a vast and constantly expanding market. Large numbers of online and offline users are now transacting through various modalities such as net banking, mobile banking, mobile wallets, credit/debit cards, etc. due to the spread of digital banking systems and financial inclusion policies in India. According to RBI data, bank deposits increased at a CAGR of 11.11% from FY09 to FY17, reaching $1.86 trillion in USD by FY19. As of February 2020, deposits totaled $1893.77 billion [9]. The graph (Table 1) below provides statistical information about the quantity and value of transactions made through different channels as of May 2020[9]. Banks are extremely vulnerable due to their extensive business operations, high volume of financial transactions, large volume of data and information about a large clientele, and absence of a robust, multi-layered security system. Data loss and financial loss account for 88% of the effects of cybercrime on banks, according to research. Cyberattackers' goals aren't always to steal money or create other financial losses; on occasion, they aim to obtain financial and personal information in order to obtain knowledge about other company models and customer information . Because of their concern for data security, banks may lose a significant portion of their client base and face reputational damage as a result of this espionage.

Transactions and Value of Transactions through Various Modes as of May 2020

The Indian banking system has previously been the target of numerous cyberattacks that attempted to steal money or cause financial damage. As a result, there were significant operational, financial, and reputational consequences, as well as losses to clientele and personal data. According to RBI data, there were 13,083 and 11,997 cases of online banking fraud and ATM, credit, and debit card fraud in 2014–15 and 2015–16, respectively . In addition, data collected by CERT-in indicates that 44,697 and 49,455 cyber security cases pertaining to phishing, malicious programs, denial of service, website hacking, etc. were reported in the years 2015 and 2016, respectively (Buletin, 2020). When compared to earlier times in India, there is a rise in the quantity of these cases nowadays. A number of high-profile cyberattack cases against the Indian banking sector have resulted in significant financial losses and exposed the bank to excessive risk from its current clientele. Among them were a phishing attempt to steal $170 million from Union Bank of India in 2017 and a malware attack that stole 94 crore from Cosmos Bank Pune's switching system in

August 2018. the largest cyberattacks in Indian history include the phishing attack on UTI bank on February 14, 2007, the SIM Card swap fraud cases that resulted in the loss of 4 crores and numerous customers, the hacking of the ATM system in Kolkata that caused a loss of 20 lakhs rupees and other website hacking cases, and the busting of a racket including an online misrepresentation worth Rs 12.5 lakh by the Rourkela police.

In order to identify systemic vulnerabilities and provide optimal preventative actions to shield the system from future cyberattacks, this article includes case study data from two of the aforementioned cyberattacks.

Case of Cyber-Attack on UBI 2017

The 2017 UBI cyberattack is a prime example of phishing, initiated by a spoof email purporting to be from the most reliable source, the Reserve Bank of India. A small number of customer care, individual, and e-banking email addresses received the dangerous code-laden email. Few individuals in total reported the email to the bank's security personnel. They believed that even though the email came from RBI, there may have been some misgivings about its substance because it contained a.xer file rather than a pdf or xls. Unfortunately, a small number of unsophisticated individuals did open the email, and shortly after, malicious malware infiltrated the bank's servers and network, allowing hackers to attempt a $170 million robbery. However, during the process of reconciling their Nostro account, the attackers made the little error of erasing the transactions from SWIFT files, which were discovered by the Treasury Department in the backend.

What then went wrong in this instance? Despite the bank's infrastructure having all the necessary safeguards in place, attackers were nevertheless able to find a weakness and establish a foothold by breaking into the system. The primary intent behind this attack was money theft and the acquisition of financial information. Therefore, the first issue that has to be addressed is a lack of knowledge about cybercrime and inadequate training for officials to recognize cyberattacks early on and stop any such losses.

A Comparison of no of cyber cases between nationalized banks and private sector banks between periods 2017-18 and 2018-19.

In addition to the two case studies mentioned above, this research study contrasted the number of cyberattacks that occurred in nationalized and private sector banks between 2017–18 and 2018–19 [9].The research below is limited to Indian banks once more. The data shown in Table 2 suggests that the percentage increase in fraud cases within private sector banks is lower than that of public sector banks. Additionally, the amount of fraud involved in public sector banks has increased at a faster rate than that of private sector banks. This huge difference could be caused by a number of factors. Private sector banks allocate a significantly larger portion of their budget to cyber security measures such as establishing multilayer, highly secure environments, safeguarding data and information, updating outdated environments with the newest hardware and software, and putting in place an appropriate security framework that continuously monitors and advises the bank environment, conducts audits at predetermined intervals, and offers security solution training.

Frauds in Private Sector and Public Sector Banks

Results and Findings

Phishing, identity theft, and malware are the main causes of crimes in the Indian banking industry.

Ignorance of cyber security policies and simple mistakes can lead to major crimes as well. Before taking any action, suspicious items should be carefully handled and the relevant authoritiesnotified. Systems must to undergo audits at regular intervals to check for security breaches.

It is recommended that public sector banks prioritize improving security through public-private partnerships and spend additional funds towards data protection and security framework enhancement.

ATM/POS machines switching system connectivity with core banking system should be continuously monitored along with ATM/POS machine transaction monitoring. A constant network packet as acknowledgement signal should be sent and received between to validate connectivity

Safety Mechanism

As technology advances, cyberattack methods are evolving as well. In order to successfully obtain privileges and cause disruptions to the network, attackers have gotten more skilled at identifying, gathering, and evaluating vulnerabilities as well as gaps in the system. Banks are now implementing the newest cyber-security technology and are willing to pay more money to secure their environment from unauthorized access, unneeded data breaches, and security lapses in order to become well-aware of and advanced with the current hacking techniques. A firewall that is configured and maintained properly helps shield the banking environment from unauthorized attacks.

Banks should use a variety of safety precautions to thwart any such known cyberattacks. A test known as a penetration test is used in bank premises to evaluate the security of the network and infrastructure of banks. Its goal is to uncover system vulnerabilities and breaches by having the tester pretend to be an intruder and attempt to penetrate the security system[15].Numerous such tests have been conducted in the past, and based on the information gathered from those tests, it was discovered that the majority of vulnerabilities discovered in Indian banks are related to web applications, inadequate network security, ineffective password management, incorrect server configuration, and ignorance.

The usage of the secret socket layer (SSL) protocol is one of the required methods to avoid cyber-attacks against bank backend online services. Any browser that requests access to a website's data does so by first retrieving the SSL certificate and verifying that it is valid, issued by a recognized authority recognized by the browser, and being used by the website for which it is intended. If all of these conditions are met, the browser is then granted access to the website's data.

It may be simpler for attackers to gain access to the network and server levels when password management is inefficient. Strong passwords need to be handled, changed on a regular basis, and kept in a suitably protected and encrypted manner. Encrypting passwords at every security level is essential. Passwords should be securely encrypted and should not be visible anywhere within the system. To access any password, the encryption and decryption methods have to be adhered to. Anywhere that a password is hardcoded, it can be encrypted and stored in a configuration file, which can then be accessed from anywhere in the code. In order to decrypt the password using logic, the decrypt key file is utilized to store the key simultaneously. To better guard against source code manipulation, this setup can be completed with ease. An improved solution for login-related problems is to use two-factor or multi-factor authentication.

Firewall settings are required to protect networks. As seen in the above diagram, several tiered protection frameworks ought to be suggested in order to secure the system core. Firewalls and traffic content filters are essential for preventing unauthorized and undefinable material from entering the top network layer. Antivirus software should be used to direct the platform layer underneath. Updates and patches for operating systems and other software should be applied on a regular basis. Outdated hardware and software should be swapped out for the newest models with improved security fixes. The foundation of back office IT is comprised of numerous lines of source code found in the application layer. The framework for necessary preventive must be used to safeguard the source codes. To protect their software, developers must implement password encryption and reduce vulnerabilities associated to their code. For auditing purposes, files and data must also be encrypted and safeguarded.

A survey about the safety precautions taken by a few Indian banks to safeguard the environment was conducted. The majority of banks have implemented password encryption and other preventive measures as previously mentioned, but there are programs in place to ensure minimum user awareness. A small sample of people was surveyed regarding cyber security, and the results showed that only 5–10% of respondents were aware of policies and security awareness, while the majority of respondents knew very little or nothing at all.

It was discovered that just a small number of banks allocated the proper funds for information security awareness and data protection initiatives. Maintaining data confidentiality is the duty of every individual in an organization. In the picture below, sensitive data is categorized in depth.3. Everyone should be well-versed in protecting breaches of extremely sensitive data; otherwise, a single human error could put the bank at danger.

Conclusion and Future Scope

Cybercrimes are unrestricted and develop at a rate that keeps up with new technological advancements. An very real threat to banking and financial institutions is the unprecedently high increase of cybercrime and its catastrophic effects. It attempts to create a lively security readiness among banks and other financial institutions. The increasing reliance of billions of people on e-banking technology at various levels presents a significant challenge to cyber professionals in developing a robust cyber security protocol.

In addition to combating cyber weaknesses, Indian banks must also change their mentality and become psychologically ready to respond to cybercrimes and criminals like they would in a battle. The traditional methods that have been used throughout should be dropped in favor of cutting-edge technologies that offer nimble and unconventional means of combat. Reviewing the state of cyber security and new threats is also necessary.

Indian banks are the backbone of the nation’s economy and a tool available to both individuals and institutions. It is imperative that a bank maintains its sound financial institution and credibility at all costs. The moment has come for banks to abandon their conventional banking structures and collaborate with new technologies and innovative ideas to eliminate or significantly reduce the cyber threat within the system.

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. 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.
3. 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.