DE JURE NEXUS LAW JOURNAL

Author:

Shreya Mishra

Symbiosis Law School, Noida

2nd Year, BBA LL.B.

CYBER SAFETY OF NATIONALISED BANKS OF INDIA

Abstract-

The world is digitalizing and so is the banking sector. Internet banking is now one of the fastest and easiest way of banking. But the sophistication, frequency, and severity of cyberattacks has grown too. Cyber-attacks are targeting the security of these financial institution. There is a growing need for banks in India to withstand, recover and adapt to changing technology. The surge in digitalization has led to a spike in cyberattacks as cybercriminals are able to find new vulnerability in the existing institution. As of August, 2021 India has 12 nationalised banks and Reserve bank of India is the governing body. Almost all these banks in India have started the process of digitalization but the challenge is currently they are at varying stages of digital transformation. Cyber safety in Financial institution is protection of a user's money, login credentials and sensitive information from cyber criminals.

Introduction

This research paper explores the journey of cybercrime from the point it was invented to current scenario of cyber-crime related to banks. We will analyse the nature of cybercrimes in banking sector. We will see what are the challenges faced by this sector. We will also look at the techniques used by cyber criminals to commit the crimes. Finally, we will look at set of suggestions that a used should follow in order to avoid to be victim of cybercrime. We will also look the course of action a user should take after finding himself as victim of cyber-crime.

Looking behind and Current Scenario

The first virus was discovered in 1971 called Creeper and reaper. During 1990s the concept of antivirus, firewall, email security came into picture. Towards the 2000s, awareness grew regarding Data Protection, data encryption and Intrusion Detection System and Intrusion Prevention System. Data theft at Zomato in 2017 startled many across the globe. In 2017-18, World's biggest ransomware attack 'Wanna Cry' and 'Notpetya' was reported which costed at least US$ 10 billion. It affected banks, ATM networks, and card payment systems. In the same year A Pune-based leading cooperative bank lost US$ 13.8 million in cyber-attacks. Global rating agency Moody's Investors Service has warned banks of increased risks of cyberattacks

during the ongoing covid-19 pandemic[1]. The national security advisor affirmed that "financial frauds increased exponentially due to greater dependence on digital payment platforms following the COVID-19 pandemic".

Nature of attacks

There are basically three types of cyber-attacks.[2] The first one is Man-in-The-Middle attacks. Here the cyber-criminal attacks the compromised personal routers to conduct the Distributed Denial of- Service (DDoS) attack, financial fraud, as a hop point to conceal original attack location. The second one by disrupting the services and abusing the login credentials of the victim's anomalous locations using stolen credentials. And the last one is phishing and social engineering attacks. Here the information is stolen by fraudulently stolen by pretending to be legit on the face. Bogus websites, fake online platforms, spam, phishing e-mails tend to lure potential victims. These only require remote workforce, so are relatively easier to execute.

Challenges

Banking is an employee-intensive industry and maintains a high touch customer-service model. The online environment affects the operational activity of bank. Bank has to deal with myriad of customers with different knowledge and inclination to use digital platforms. Furthermore, the pandemic has worsened the situation as the senior customers preferred physically going to the bank.

In today's world cyber-crime is beyond data leakage and lack of access control but more about using and selling the data or siphoning off funds. Digital identities are often getting cloned. Cyber criminals are capable of data theft, money laundering through various software programmes and network algorithms.

Banks are prime target as they deal with Personally Identifiable Information (PII) and financial data. The key issue is Data sharing mechanisms. They require customer's consent. The RBI has acknowledged and envisaged an account aggregator (AA ecosystem) platform to deal with the challenge. These Aggregators are responsible for transferring data without storing it [3].

The ecosystem of banking is highly integrated and require third-party vendors for operations. These vendors have access to banks network, this implies that anyone vulnerability in this infrastructure could risk the security of a bank.

Tracking cyber criminals is extremely difficult because the technique used by them are continuously evolving. Tracking the origin of the crime is difficult because the criminal investigation and the criminal activity itself is borderless by nature. Shortage of skilled cyber-

[1] Read more at: https://economictimes.indiatimes.com/industry/banking/finance/banking/moodys-warns-banks-of-increased-cyber-risks/articleshow/76856381.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

2 Cybersecurity in the Indian banking industry: Part 1 Will 2020 redefine the cybersecurity ecosystem?,

https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-cybersecurity-in-the-indian-banking-industry-noexp.pdf

[3] Reserve Bank of India, "Master Direction: Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016", Master Directions, September 02, 2016 and updated on November 22, 2019, https://m.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598

crime fighters along with lack of proper devices hamper the process of investigation. The shortage of cybersecurity workforce is worldwide. The survey conducted by the Information Systems Audit and Control Association (ISACA) says that the majority of the respondents reported that their cybersecurity teams were understaffed and they faced resourcing and retention challenges. According to Data Security Council of India (DSCI) predicted in 2015 that India will need one million cybersecurity professionals by 2020[4]. The widespread use of pirated software adds fuel to fire. These pirated softwares are prone to attacks by virus, malware and trojans. Unmonitored and insure home Wi-fi network coupled with lack of awareness can be easily targeted.

Laws governing Cyber space in India

In India the main governing legislation is the Information Technology Act, 2000. This act defines cybersecurity defines cybersecurity as protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction. Along with legal recognition and protection for electronic transaction, Information and Technology Act also redefines the role of intermediaries, recognizes the role of the Indian Computer Emergency Response Team ("CERT-In") etc. The of IT Act has also amended the scope Indian Penal Code, Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, and the Reserve Bank of India Act, 1934 to focus on target regulation and reporting of cyber-crimes. The IT Act prescribes penalties starting from fines to imprisonment for various kinds of malicious cyber activities, including hacking, tampering with computer source code, denial-of-service attacks, phishing, malware attacks, identity fraud, electronic theft, cyberterrorism, privacy violations and the introduction of any computer contaminant or virus[5]. Section 66 of the IT Act provides for punishment in the form of imprisonment for a term up to three years or a fine of up to INR 500,000 if a person dishonestly or fraudulently commits any offence under Section 43 of the IT Act, including: hacking (i.e., accessing a computer, computer system or computer network without the permission of the owner, or downloading, copying and extracting any data, or disrupting any system); injection of malware into a computer; and denial-of-service attacks (i.e., denying access to any person authorised to access a computer) and the like. Section 66C of the IT Act provides that anyone that fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person shall be punished with imprisonment of up to three years and may also be liable to be punished with fine of up to INR 100,000.

Preventive measures

A very serious challenge against fighting cyber criminals is preventing them from damaging the existing infrastructure. But certain precautionary measures are pertinent. Using a secure network helps in making the user less vulnerable cyber threats. A user should maintain up to date operating system on computers. A person should be extremely careful while using confidential information on online platform related to bank. Avoid clicking on e-mails which

[4] Data Security Center of India, "Cyber security: 1 million cyber security professionals needed by 2020", Press Release, DSCI News Center, August 2015

[5] Read on: https://www.mondaq.com/india/technology/963026/cybersecurity-comparative-guide

are spammed and looks shady. While using online payment mode through credit or debit cards make sure that the website is asking for OTP. Avoid saving and sharing credit card information on digital devices. Notify the bank immediately if you find something suspicious. Monthly credit card statement should be done carefully without fail.

Not only users but Banks too need to fulfil regulatory requirements and improve their cyber defence system. They should be prepared for any kind of expected and more sophisticated attacks. Banks ought to be proactive while handling the data of a user. Monitoring, resolving, enhancing the digital platforms but antivirus programmes, firewalls and other encryption tools. Banks need to comply with the RBI guidelines on cyber security frameworks which focuses on cyber security and resilience, cyber security operations centre, cyber security incident reporting. Banks should approach though a continuous threat assessment-based risk management system. The bank should take the responsibility of educating the end user about importance of protecting the information in order to avoid cyber-attack. They can organise training programmes. They should also tighten the access to third-party service providers by restricting or controlling access to sensitive information. Banks are also engaging vendors to conduct mock cyber-attacks on their platforms to see whether their defences are breached — and to find loopholes and plug them.[6]

Conclusion

In this era of digitalisation cyber-crimes are rising tremendously. Thanks to Covid-19 which has accelerated both the digitalization and incidents of cyber-crimes. Banks are likely to adopt technologies such as mobile, cloud, remote access, and IoT, not out of choice but out of the need to sustain business during the pandemic and thrive thereafter. The internet is the medium for huge information and medium of communication around the world, it is necessary to take certain precautions while using it for financial transactions

[6] Read on: https://economictimes.indiatimes.com/industry/banking/finance/banking/banks-rope-in-global-cos-to-guard-against-rising-cyberattacks/articleshow/84904963.cms