WEB OF SYNERGY:
International Interdisciplinary Research Journal
Volume 2 Issue 1, Year 2023 ISSN: 2835-3013
https://univerpubl.com/index.php/synergy

Cyber Security Challenges in Indian Banks

Ekta Dureja
Assistant Professor, Department of Computer Science, S.D. (PG) College, Panipat, Haryana, India

Article Information

Received: November 02, 2022
Accepted: December 01, 2022
Published: January 31, 2023

Keywords: *cyber security, banks, technology, challenges and cyber crimes.*

ABSTRACT

As we transition to a digital economy, cyber security in banking is becoming a serious concern. Utilizing methods and procedures created to safeguard the data is essential for a successful digital revolution. The effectiveness of cyber security in banks influences the safety of our Personally Identifiable Information (PII), whether it be an unintentional breach or a well-planned cyber attack. The stakes are high in the banking and financial industries since substantial financial sums are at risk and the potential for significant economic upheaval if banks and other financial systems are compromised. With an exponential increase in financial cyber security, there is high demand for the profession of cyber security. This research paper focuses on the cyber security issues faced by Indian banks. It also helps to analyse about the awareness of Cyber crimes to the common people.

INTRODUCTION

The arrangement of technologies, protocols, and methods referred to as "cyber security" is meant to guard against attacks, damage, malware, viruses, hacking, data theft, and unauthorized access to networks, devices, programs, and data. Protecting the user's assets is the primary goal of cyber security in banking. As more people become cashless, additional acts or transactions go online. People conduct transactions using digital payment methods like debit and credit cards, which must be protected by cyber security.

During the ongoing COVID- 19 pandemic world is going through a change leading all the countries to take a step towards the digital area which is needed. But as a society that runs largely on technology, we are also as a result dependent on it. And just as technology brings ever greater benefits, it also brings ever greater threats. It becomes a focal point for cybercrime. RBI published Technology Vision for Cyber Security for Urban Cooperative Banks 2020- 2023 The Reserve Bank of India has today placed on its website the Technology Vision for Cyber Security for Urban Co-operative Banks (UCBs) 2020-2023. The Technology Vision Document aims at enhancing the cyber security posture of the Urban Co-operative banking sector against evolving IT and cyber threat environment.

The year 2020 has been quite challenging for Indian banks when it comes to cyber security. After the onset of the COVID-19 crisis, banking operations disrupted severely as banks struggled to provide uninterrupted services to their clients during various stages of lockdowns. In the following months, they accelerated their digital transition efforts (such as digital banking and remote access to employees) to ensure contactless business operations. With a surge in digitization, banks also witnessed a spike in cyber attacks as cybercriminals found new

opportunities and vulnerabilities. Indian banks are likely to continue to experience rising financial frauds due to the increasing digital attack surface. Rising cyber threats after COVID-19 pose serious concerns for Indian banks and the Reserve Bank of India (RBI). Areas under cyber security: Cyber security or information technology security are the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation.

SCOPE OF THE STUDY

The banking sector is a major contributor to the growth of the Indian economy. Since late eighties, the Indian banks have been aggressive in implementing technological solutions. This has caused major concerns in terms of protecting and preserving the privacy of information assets throwing numerous risks to banks and customers. Numerous studies across the world have emphasized the need and requirements for detailed analysis on Cyber security issues in banking. The Indian banks unlike foreign banks are huge in size and have a large number of human assets and branches. Hence, managing Cyber security in these larger organizations is challenging and mandates for effective risk management. Therefore, the present study on Cyber security threats in the Indian banks has high relevance in the modern day business environment.

LITERATURE REVIEW

Arief R. et al. (2011) Group of Faculty of computer science from university of Indonesia specifically discusses about three types of applied ethics i.e. Cyber ethics, information ethics and computer ethics. There are two aspects of these three applied ethics that is there definitions and the issues associated with them. Authors also say that these three applied ethics acts as a base for e-government ethics and can enrich the e-governance of the country.

Ashwini B. (2012) Author discusses broadly about the ratio of increasing cyber crime and their effect on the society and e business and retailers. The paper briefs about the cyber threat and frauds, it also briefs about the internet user in India, its scope and future. Author also puts light on the governmental measures to stop cyber crime and talks about the challenges that India needs to face to beat cyber threat.

Bawa D. and Marwah D. (2011) Authors explain in this Cyber ethics refers to the code of responsible behaviour on the internet, this paper explores the codes of online conduct that are emerging as new media gains more influence in political and business affairs.

Brar et al. (2012) In their study on vulnerabilities in the security aspects of e-banking, observed that use of internet technologies have transformed banking industry from the customer and bank perspectives. The study further pointed out that it has greatly increased the number of criminal activities like customer identity theft, phishing, DOS attacks, malware attacks; ATM related cyber threats and credit card based cyber frauds.

Cezar V. (2012) This paper explores the notion of cyber attack as a concept for understanding modern conflicts. Author elaborates a conceptual theoretical framework, observing that when it comes to cyber attacks, cyber war and cyber defence there are no internationally accepted definitions on the subject.

National Cyber Security Policy Govt. Of India (2011) In this paper gives a detailed study about the cyber security, cyber space and its strategic perspective authors also explain that legal framework, law enforcement and information sharing. Paper also talks about the awareness created at different level of users (corporate, home users, students etc) through training. The paper is concluded by discussing the technologies used for ensuring security.

Sanjay P. (2010) Author discuss in detail the provisions of IT Act, 2000 and its recent amendments towards combating cyber crime. Author has also made an attempt to analyse the current trends in cyber crime then the analyses is made on the needs of legislation and current

provisions of IT Act, lastly paper talks about similar provisions in the world and drawing parallel laws in the country. Finally author sums up the discussion with suggested recommendations for possible and safe cyber world.

Samridh S. et al. (2012) The paper proposes a curriculum for cyber safety education in schools. The proposed curriculum covers four sections: Cyber Threats, Protecting Ourselves, Cyber Ethics and Cyber Laws.

OBJECTIVES OF THE RESEARCH

1. To find out the attitude of people towards adoption of cyber security in India.

2. To understand the Cyber security threats (challenges) faced by the Indian banks.

3. To offer suitable suggestions in handling cyber issues in banking sector.

RESEARCH METHODOLOGY

The research study has been done from secondary data through various websites, journals and reference books. Primary data is also collected from a sample size of 50 respondents to evaluate the awareness of common people with respect to the cyber security challenges.

MAJOR AREAS COVERED IN CYBER SECURITY

1. Application Security:- It encompasses measures or countermeasures that are taken during the development life-cycle to protect applications from threats that can come through flaws in the application design, development, deployment, upgrade or maintenance.

2. Information Security:- Information security protects information from unauthorized access to avoid identity theft and to protect privacy. Major techniques used to cover this are: a) Identification, authentication & authorization of user

3. Disaster Recovery:- Disaster recovery planning is a process that includes performing risk assessment, establishing priorities, developing recovery strategies in case of a disaster. Any business should have a concrete plan for disaster recovery to resume normal business operations as quickly as possible after a disaster.

4. Network Security:- It includes activities to protect the usability, reliability, integrity and safety of the network. Effective network security targets a variety of threats and stops them from entering or spreading on the network.

NETWORK SECURITY COMPONENTS

India has seen a series of unprecedented events during the last one year, which have brought the issue of cyber security for the Indian banking sector to the fore like never before. The most significant factor in this regard has been the ongoing initiative of the Government of India, through its flagship Digital India programme with a vision to transform India into a digitally empowered society and knowledge economy. The sharp rise in value and volume of digital transactions which touched record levels in March 2017 manifests the accelerated shift towards electronic payments. The continued increase in penetration of inclusive banking through the Pradhan Mantri Jan Dhan Yojana (PMJDY) with the total number of accounts crossing 29.18 crore brought the uninitiated and new users into the fold of banking services. Two of the major events included the compromise of the SWIFT payment application in a major bank and subsequent large value fraudulent fund transfer and the large scale compromise of debit cards of multiple banks, via an advanced and persistent attack on a payment processor . As famously stated by Nicholas Carr, When a resource becomes essential to competition but inconsequential to strategy, the risks it creates become more important than the advantages it provides. Cyber risk now ranks among the existential risks for Indian banks.

TECHNOLOGY LANDSCAPE

The pace of digitization of financial transactions in India continues to gather pace. It is estimated that noncash payment transactions, which today constitute 22 percent of all consumer payments, will overtake cash transactions by 2023.The technology infrastructure continues to build up, with 100 crore mobile connections in the country, of which 24 crore are of Smartphone users. The number of smart phones has increased to 52 crore by 2020. Around 90 percent of all devices are internet enabled and the number of internet users has doubled to nearly 650 million by 2020 from 300 million in 2015.

Meanwhile, the Aadhaar enrolments continue to reach saturation levels, with two states already reporting 100% coverage. The PMJDY accounts extended the financial inclusion agenda, with almost 18 crore accounts being in semi-urban/rural areas. It needs to be kept in mind that most of these account holders will be new to the banking processes and the technology infrastructure underlying it, making them vulnerable to social engineering and other cyber attacks.

CURRENT STATE OF CYBERSECURITY IN BANKS

Between June 2018 and March 2022, Indian banks reported 248 successful data breaches by hackers and criminals; the government notified Parliament on Aug 2, 2022.

The Indian government has reported 11,60,000 cyber-attacks in 2022. It is estimated to be three times more than in 2019. India has been the target of serious cyber attacks, such as the phishing attempt that nearly resulted in a $171 million fraudulent transaction in 2016 against the Union Bank of India.

Another instance of a cyber attack involving online banking was Union Bank of India, resulting in a substantial loss. One of the officials fell for the phishing email and clicked on a dubious link, which allowed the malware to hack the system. The attackers entered the system using fake RBI IDs.

Banks have been mandated to strengthen their IT risk governance framework, which includes a mandate for their Chief Information Security Officer to play a proactive role in addition to the Board and the Board's IT committee playing a proactive role in ensuring compliance with the necessary standards.

TOP CYBERSECURITY THREATS FACED BY BANKS

Cybercrimes have increased frequently over the past several years to the point where it is thought that they are one of the most significant hazards to the financial sector. Hackers have improved their technology and expertise, making it difficult for any banking sector to thwart the attack consistently. The following are some dangers to banks' cyber security:

1. Phishing Attacks: One of the most frequent problems with cyber security in the banking sector is phishing assaults. They can be used to enter a financial institution's network and conduct a more severe attack like APT, which can have a disastrous effect on those organizations (Advanced Persistent Threat). In an APT, a user who is not permitted can access the system and use it while going unnoticed for a long time. Significant financial, data and reputational losses may result from this. According to the survey, phishing assaults on financial institutions peaked in the first quarter of 2021.

2. Trojans: The term "Trojan" is used to designate several dangerous tactics hackers use to cheat their way into secure data. Until it is installed on a computer, a Banker Trojan looks like trustworthy software. However, it is a malicious computer application created to access private data processed or kept by online banking systems. This kind of computer program has a backdoor that enables access to a computer from the outside.

Around the globe, there were roughly 54,000 installation packages for mobile banking trojans in the first quarter of 2022. There has been an increase of more than 53% compared to last year's quarter. After declining for the first three quarters of 2021, the number of trojan packages targeting mobile banking increased in the fourth quarter.

3. Ransomware: A cyber threat known as ransomware encrypts important data and prevents owners from accessing it until they pay a high cost or ransom. Since 90% of banking institutions have faced ransomware in the past year, it poses a severe threat to them.

In addition to posing a threat to financial cyber security, ransomware also affects crypto currency. Due to their decentralized structure, crypto currencies allow fraudsters to break into trading systems and steal money.

4. Spoofing: Hackers use a clone site in this type of cyberattack. By posing as a financial website, they;

- Design a layout that resembles the original one in both appearance and functionality
- Establish a domain with a modest modification in spelling or domain extension

The user can access this duplicate website via a third-party messaging service, such as text or email. Hackers can access a user's login information when the person is not paying attention. Seamless multi-factor authentication can solve a lot of these issues.

The Reserve Bank of India (RBI) reported bank frauds of 604 billion Indian rupees in 2022. From more than 1.3 trillion rupees in 2021, this was a decline.

CYBER SECURITY CHALLENGES

Some of the factors which continue to have their impact on the state of cyber security are low awareness.

1. Awareness remains low: Awareness amongst internal employees remains the first line of defense. However, not many firms invest in training and improving the cyber security awareness levels within the enterprise.

2. Inadequate Budgets and Lack of Top Management support: Budgets are usually driven by business demands and low priority is accorded to Cyber security. Top management focus also remains a concern, support for cyber security projects are usually given low priority. This is primarily due to the lack of awareness on the impacts of these threats.

3. Poor Identity and Access Management: Identity and access management is the fundamental element of cyber security. In an era where hackers seem to have upper hand, it requires only one hacked credential to gain entry into an enterprise network. Despite some improvement, there remains a lot of work to be done in this area.

4. Ransomware on the Rise: The recent episodes of malware attacks, viz. WannaCry and Petya, brought home the rising menace of ransomware. As more users recognize the risks of ransomware attack via email, criminals are exploring other vectors. Some are experimenting with malware that reinfects later, long after a ransom is paid, and some are starting to use built-in tools and no executable malware at all to avoid detection by endpoint protection code that focuses on executable files. Ransomware authors are also starting to use techniques other than encryption, for example deleting or corrupting file headers.

5. Mobile devices and Apps: As organizations move towards adopting mobile devices as its preferred channel for doing business, it also becomes the ideal choice for hackers to exploit as the base increases. Since financial transactions can be done on mobile apps, the mobile phone is becoming an attractive target leading to an increase in mobile malware. The risk of jail-broken and rooted devices used for financial purposes increases the scope of attack.

6. Distributed denial of service (DDOS) attack: With the advent of IOT-powered botnets, destructive DDOS attacks are inevitable and have intensified in volume and frequency. Organizations in India need to improve their response capability to mitigate DDOS risks.

7. Social Media: Growing adoption of social media leads to more potential for hackers to exploit. Many a user puts her data out for anyone to see, which can be potentially exploited to attack the user_s organization. Use of social media to propagate fake news can impact banks_ reputations in an insidious manner.

APPLICATIONS OF CYBERSECURITY IN BANKING

Cyber security threats are constantly evolving, and the banking sector must take action to protect itself. Hackers adapt when new defenses threaten more recent attacks by developing tools and strategies to compromise security. The financial cyber security system is only as strong as its weakest link. It is critical to have a selection of cyber security tools and approaches available to protect your data and systems. Here are a few crucial cyber security tools:

1. Network Security Surveillance: Network monitoring is known as continuously scanning a network for signs of dangerous or intrusive behavior. It is frequently utilized with other security solutions like firewalls, antivirus software, and IDS (Intrusion Detection System). The software allows for either manual or automatic network security monitoring.

2. Software Security: Application security safeguards applications that are essential to business operations. It has features like an application allowing listing and code signing and could help you synchronize your security policies with file-sharing permissions and multi-factor authentication. The use of AI in cyber security will inevitably improve software security.

3. Risk Management: Financial cyber security includes risk management, data integrity, security awareness training, and risk analysis. Essential elements of risk management include risk evaluation and the prevention of harm from those risks. Data security also addresses the security of sensitive information.

4. Protecting Critical Systems: Wide-area network connections help avoid attacks on massive systems. It upholds the rigid safety standards set by the industry for users to follow when taking cyber security steps to protect their devices. It continuously monitors all programs and performs security checks on users, servers, and the network.

CYBER SECURITY INITIATIVES IN INDIA

ISO 27001 (ISO27001) is the international Cyber security Standard that provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System.

INDIA'S LEGAL FRAMEWORK FOR CYBER SECURITY

1. Indian IT Act, 2000 Section 65 - Tampering with computer source code, Section 66 - Hacking & computer offences, Section 43 – Tampering of electronic records

2. Indian Copyright Act States any person who knowingly makes use of an illegal copy of computer program shall be punishable. Computer programs have copy right protection, but no patent protection.

3. Indian Penal Code Section 406 - Punishment for criminal breach of trust and Section 420 - Cheating and dishonestly inducing delivery of property.

4. Indian Contract Act, 1872 Offers following remedies in case of breach of contract, Damages and Specific performance of the contract.

DATA ANALYSIS AND INTERPRETATION

For Data Analysis and Interpretation the survey of fifty respondents was done through Google form.

- Maximum respondents 34 were male, only 15 were female 40 respondents belong to the age group of 18 to 30 years. 5 respondents were from 30 to 40 age group and 3 respondents are from under 18 age group and 1 respondent is from 40 to 50 ages group.1 respondent was from 50 above age group. Maximum respondents belonged to students group.
- There were mix responses about using online banking system in their day to day life. 44 respondents use online banking system in their daily life. 5 respondents do not use online banking system due lack of security issues. 1 respondent is not sure about using online banking system.
- Out of 50, 47 respondents had a bank account.
- With respect to mode of payment used the analysis was as follows 14 respondents still trust on cash payment for their workings. Debit and Credit Cards are used by 13 and 2 respondents respectively. Internet banking is being used by 5 respondents. Mobile banking is being used 11 respondents. Cheque and e -wallets are used by3 and 2 respondents respectively. We can see there is increase in use of mobile banking in Indian banking customers.
- Out of 50, 36 respondents are aware of cyber crimes. Remaining are not aware or not sure.
- With respect to awareness about various cyber crimes 19 respondents heard about hacking it is most known cyber crime people aware of. 16 respondents heard about banking / credit card related crimes in Indian banks which they are aware through different mediums.
- 16 respondents think that cyber security issues are main reason because of which there banks accounts are not secured. 11 respondents think that fraud exposure in banks is the reason. Virus attacks and internet related threats are distributed equally i.e 10 respondents respectively. 3 respondents think that management related threats are also the reason.
- 9 respondents believe that covid-19 is the factor due to which they started using online banking.
- 35 respondents have trust on public sector banks. 11 respondents have faith in private sector banks.
- 12 respondents are not at all aware about cyber security issues which show lack education and awareness.
- Most dangerous cyber attacks for Indian banks. 16 respondents feels that stolen of confidential data is the most dangerous cyber attack for Indian banks. 12 respondents feels that Data corruption which comes second most dangerous cyber attack . Malware attacks and identity theft are 5-5 respondents respectively.
- With respect to best security tools to protect online banking; 23 respondents thinks that biometrics- retinal scan of fingerprints, voice etc is the best tool to protect online banking. 16 respondents feel that passwords enable to protect online banking. 7 respondents feel that Digital electronic signature is best tool for protection of online banking. 4 respondents' feels that digital electronic certificates are best tool.
- 23 respondents are aware about cyber security protection act.
- 35 respondents have not experience any cyber threat. 9 respondents have experienced cyber threat in their life. 6 respondents prefer not to say about their experience.

CONCLUSION

Every organization is concerned about cyber security. It is crucial for banks to have the proper cyber security solutions and procedures in place, especially for institutions that store a lot of personal data and transaction lists. Banking cyber security is an issue that cannot be bargained with. Hackers are more likely to target the banking sector as digitalization advances.

Banks should look after cyber security issues in their online banking facilities. There are customers who have bank accounts but not aware about cyber crime and attacks related to it, and what harm it can cause to them. Most of the people believe that cyber Protection Act is important for Indian banks. Most of the people are using online banking system which leading India to digitalization. In the pandemic situation of covid19 digital payments have helped a lot.

Hacking and banking/ credit card related cyber crimes are most common cyber crime that people are aware of. Privacy and security is reason which influences people towards online banking. There are people who still don't have bank accounts. Banks cyber attacks increased 238% during February-April 2020. Reserve Bank of India had set up Reserve bank information technology Private limited (Rebit) to take care of IT requirements and cyber security in Indian banks.

People are still in favour of cash payments for their day to day life. Banks should do education and awareness program for their customers. People do not have trust in private sector banks and foreign banks as compared to public sector bank in India specially. Central government must enhance cyber hygiene among all end-users and to create a secure and safe internet ecosystems and The Centre Emergency Response Team (CERT-In) must coordinate required tasks. Banks must practice a rigid cyber hygiene regimen to prevent malware infections on their systems and to ensure security through suitable anti-malware.

The other area that requires immediate attention is to increase insurance coverage for cyber attacks. With rise in malware attacks, banks face increasing risks in cyber space. Such attacks may lead to operational and other security interruptions. Banks has to make aware their customers about cyber attacks and measures to be taken to stay secure and not to breach any sensitive data.

REFERENCES

1. ChangsokYoo, Byung-Tak Kang and Huy Kang Kim, (2015) Case study of the vulnerability of OTP implemented in internet banking systems of South Korea‖, Multimed Tools Appl ,vol. 74, pp. 3289–3303.
2. Claessens, J., Dem, V., De Cock, D., Preneel, B., &Vandewalle, J. (2002). On the security of today s online electronic banking systems. Computers & Security, 213: 253-265.
3. Ellen Messmer (2008). First case of drive-by pharming identified in the wild‖ [Online] Available: http://www.networkworld.com/article/2282527/lan-wan/first-case-of--drive-by pharming - identified-in-the-wild.html
4. Florêncio, D., &Herley, C. 2011) Where Do All The Attacks Go? Economics of Information Security and Privacy III pp. 13-33. Springer New York.
5. G.Gopalakrishna (2011) Report of the Working Group on information security, electronic banking, technology risk management, and tackling cyber frauds‖, RBI, Mumbai, Maharashtra, January
6. Jason Milletary, Technical Trends in Phishing Attacks‖, US-CERT
7. John La Cour (2014) Vishing campaign steals card data from customers of dozens of banks [Online] http://blog.phishlabs.com/vishing-campaign-steals-card-data-from-customers-of-dozens-of-banks

8. MohdKhairul Ahmad, Rayvieana Vera Rosalim, Leau YU Beng and Tan Soo Fun, (2010) Security issues on Banking Systems‖, International Journal of Computer Science and Information Technologies, vol. 1, no.4, pp. 268-272.
9. Moore.T, Clayton.R&Anderson.R (2009). "The Economics of Online Crime", Journal of Economic Perspectives, Volume 23, Issue no.3, Summer 2009, pp.3-20.
10. Pharming‖,Wikipedia Available: https://en.wikipedia.org / wiki/Pharming#cite_note-3
11. R.P.Kaur, (2013) Statistics Of Cyber Crime In India: An Overview‖, International Journal of Engineering and Computer Science, vol.2, no. 8, pp. 2555-2559,
12. Special Advisory –Data Breach in Indian Banks, 2016 www.mitkatadvisory.com
13. Top Ten Cyber Squatter Cases Available: http://www.computerweekly.com/photostory /2240107807/Photos-Top-tencybersquatter-cases/1/ Cybersquatting-cases-Number-10-Dell.