

Safeguarding the Banking Sector using Cybersecurity Measures in the Digital Era

Snigdha Shambhavi Jha¹ and Anuradha Rao²

¹⁻²Department of Information and Communication Technology, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, India

Email: snigdha.jha@learner.manipal.edu, Anuradha.rao@manipal.edu

Abstract— In the rapidly evolving landscape of the digital era, cybersecurity has emerged as a critical concern for financial institutions. The increasing reliance on technology and digital platforms has provided immense opportunities for growth and efficiency, but the very same has also exposed banks to ever-evolving cyber threats. The topics explored delve into the importance of cybersecurity in the banking sector as well as the challenges faced by financial institutions in safeguarding their sensitive data and customer information. The research stresses the significance of customer awareness programs to empower users with knowledge on safe digital practices and recognizing potential phishing attempts. Educating customers becomes a pivotal aspect of the overall cybersecurity strategy.

Index Terms— cybersecurity, awareness, banking, digital awareness, cyber threats

I. INTRODUCTION

Safeguarding Financial Institutions, specifically Banking Sector using Cybersecurity measures is very much essential, in this Digital Era. This is a topic of research that delves into the importance of safeguarding financial institutions such as banks from ever-evolving threats in the digital age. This paper offers a deep exploration of the challenges faced by banks regarding the rather abrupt switch to digital banking on a large scale due to the pandemic and provide valuable insights into effective cybersecurity practices and strategies specifically tailored for the banking industry[1].

The problem at hand that has inspired this research paper involves the increasing vulnerabilities and cybersecurity challenges within the Indian banking sector. With the rapid evolution of technology in financial transactions, there is a pressing need to identify, assess, and mitigate risks to ensure the resilience and security of digital payment platforms, a critical concern for institutions like the State Bank of India, HDFC Bank, ICICI Bank, and multiple others.

This research paper delves into the technical problem domain of cybersecurity and digital payment security controls for Payment System Operators (PSOs), and aims to address emerging challenges and vulnerabilities in the rapidly evolving landscape of digital transactions, particularly within the context of India, shedding light on the imperative need for robust measures to ensure the resilience and security of digital payment systems. It includes identifying the threats in banking sector, finding the impact of cyber-attacks and finding the ways to establish a secure network in the financial institutions.

This research paper builds on the references taken for its creation, but also takes into account real-world examples, i.e. the customers themselves- raw and unfiltered. I have conducted a survey as part of my research during my internship at SBI, Bhopal, and its findings not only corroborate the problem statement and the underlying issues, but they also open doors into figuring out possible solutions and/or mitigating factors. They will be discussed further along.

II. THREATS IN THE BANKING SECTOR

It's important to note that cyber threats are constantly evolving, and new attack vectors emerge regularly. Banks can combat this by employing robust security measures, regularly updating systems, educating employees and customers about best practices, and collaborating with cybersecurity experts to mitigate these threats effectively.

A. Malware Attacks

Malicious software, such as viruses, worms, or trojans, can infect banking systems and compromise sensitive data. Advanced malware variants, such as banking Trojans, specifically target online banking systems.

B. Distributed Denial of Service (DDoS) Attacks

These involve overwhelming a bank's servers or network infrastructure with a flood of traffic, causing service disruptions, and rendering the system inaccessible to customers, resulting in significant financial losses and damage the reputation of the targeted bank.

C. Mobile Banking Risks

These include mobile malware, fake banking apps, and insecure Wi-Fi networks. Attackers may attempt to steal login credentials or gain unauthorized access to mobile devices to carry out fraudulent transactions.

D. Phishing Attacks

Phishing involves sending fraudulent emails or messages that appear to be from a trusted source to trick individuals into revealing their personal information, and can be highly targeted and sophisticated, making them a significant threat to banks and their customers.

III. IMPACT OF CYBER ATTACKS ON FINANCIAL INSTITUTIONS

Cybersecurity breaches can have significant impacts on financial institutions and their stakeholders, such as:

A. Financial Loss

Breaches can lead to unauthorized access to sensitive financial data, resulting in theft of funds, fraudulent transactions, or unauthorized transfers. Financial institutions may be liable for reimbursing affected customers, covering the costs of investigations, and implementing security measures to prevent future breaches[2].

B. Legal and Regulatory Consequences

Financial institutions are subject to numerous laws and regulations governing data protection and privacy, such as the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS). In the event of a breach, institutions may face legal action, fines, and penalties for non-compliance with these regulations. These legal and regulatory consequences can further impact the institution's finances and reputation

E. Operational Disruption

Cybersecurity breaches can disrupt the normal operations of financial institutions. They may need to temporarily shut down systems, suspend online services, or isolate affected networks to contain the breach. This can lead to business interruptions, loss of productivity, and delays in customer service, negatively impacting stakeholders' experience, and satisfaction.

F. Market Value Decline

Publicly traded financial institutions may experience a decline in their stock prices following a cybersecurity breach. Investors may perceive the breach as an indication of poor risk management and governance, leading to a loss of market value. This can impact the institution's ability to raise capital, attract investors, and pursue growth opportunities.

IV. ESTABLISHING A SECURE NETWORK ARCHITECTURE

Establishing a secure network architecture is crucial for banks to protect against cyber threats, which include the following:

A. Network Segmentation

Implementing network segmentation is essential to limit the lateral movement of cyber threats within the network. By dividing the network into separate segments or zones based on the sensitivity of data and systems, banks can restrict access and contain potential breaches. Segmentation can be achieved through firewalls, VLANs, and virtual private networks (VPNs).

B. Strong Perimeter Security

Banks should deploy robust perimeter security measures to protect against external threats. This includes implementing firewalls, intrusion detection and prevention systems (IDPS), and virtual private networks (VPNs) to control incoming and outgoing network traffic. Access control lists (ACLs) and network address translation (NAT) should be configured to allow only authorized traffic.

C. Robust Authentication and Access Controls

Implementing strong authentication mechanisms and access controls is critical to prevent unauthorized access to network resources. Banks should enforce strong password policies, use multi-factor authentication (MFA) for privileged accounts, and regularly review and revoke unnecessary access privileges. Role-based access control (RBAC) should be implemented to ensure employees have appropriate access rights.

D. Intrusion Detection and Prevention Systems (IDPS)

Deploying IDPS helps detect and block network-based attacks. These systems monitor network traffic, analyze patterns, and alert security teams of suspicious activity or known attack signatures. Banks should configure IDPS to generate real-time alerts and take automated actions, such as blocking or quarantining suspicious traffic.

E. Network Monitoring and Log Management

Implementing robust network monitoring and log management solutions enable banks to detect and respond to network security incidents. Network traffic should be continuously monitored for anomalies and indicators of compromise. Logs from network devices, servers, and security systems should be centrally collected, analysed, and retained for forensic analysis and incident investigation.

F. Patch Management, and Vulnerability Scanning

Banks should establish a robust patch management process to ensure that network devices and systems are up to date with the latest security patches. Regular vulnerability scanning and penetration testing should be conducted to identify and remediate any weaknesses in the network infrastructure.

G. Third-Party Risk Management

Banks should assess the security practices of third-party vendors and service providers that have access to their network. Due diligence should be conducted before engaging with third parties, and contractual agreements should include specific cybersecurity requirements and obligations. Regular audits and monitoring should be performed to ensure compliance with security standards.

V. RESULTS

Data analysis done on threats, impact of the cyber-attacks, shows the necessity of building a secure network architecture. A majority of the people who filled in these forms were employed in the public sector, comprising of almost fifty percent of the sample size population as shown in Fig1.

Thirty percent of those 150-odd people whose responses were recorded, belonged to the sector of the population still gleaning information for their careers and professional lives, i.e. students[3]. The sector that came in third in terms of most occupations taken up by applicants was that of a homemaker, comprising of about eleven percent of the sample size. Following that were people employed in the government and private sectors. Then, comprising of the minority of the sample space were people that weren't employed, or retired, or self-employed. At first glance at this aspect only, we see that a lot of the vulnerable population, that stereotypically hasn't been briefed on the

semantics of real-time cybersecurity threats, currently engage in online banking transactions, whether it be UPI (United Payments Interface), or ATM transactions.

The parameters taken to analyse based on the frequency of online banking activities done by the customer like accessing the accounts, updating the passwords in various banks. The following results show that most of the customers belong to SBI bank, accessing the accounts “very frequently and frequently”, updating the passwords “seasonally” as shown in the section A, B, C and D.

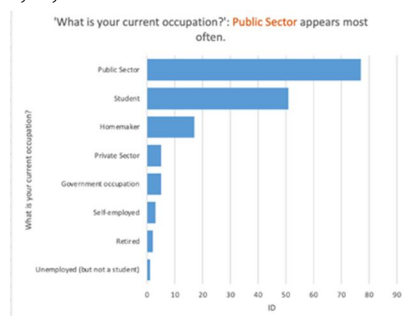


Fig.1 Current Occupation in the study

A. Frequency of Online Banking Activities

The majority answer of applicants was “frequently”, i.e. about forty-three percent of participants engaged in online banking activities fairly often, with “very frequently” coming in second, with thirty-four percent of the sample size selecting that.

After a little bit of filtering and arranging data, we see that a lot of students answered “frequently”. This only serves to further reiterate the fact that a large part of the supposedly vulnerable population engages in online transactions on a very regular basis as depicted in Fig.2

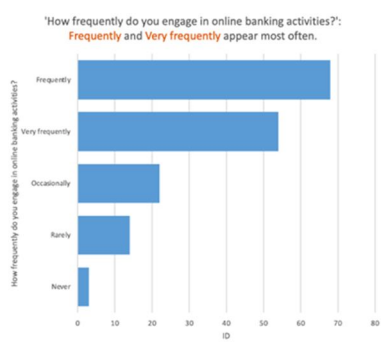


Fig.2. Online banking participation

B. Banks and their Customers

Of the many applicants that filled this form, we see a vast majority being rather loyal customers of State Bank of India, or SBI as shown in Fig.3. An overwhelming seventy percent of the people surveyed were SBI customers, while HDFC came in second place, with ten percent. ICICI and AXIS bank brought up the rear, with seven and five percent respectively. Among it, almost ten percent people said they weren’t a customer of any of the listed banks and opted for the “Other” option.

The “Other” option consisted of other primary (and majorly Indian) banks such as Bank of Baroda, Canara Bank, Federal Bank, Yes Bank, Kotak Mahindra Bank, ABN AMRO, Bank of America, IDBI Bank, BUPGB Bank, and Punjab National Bank. Additionally, while it seems to be a relief, eighty five percent of all applicants said that they were indeed aware of the security measures implemented by their respective banks to avoid any cybercrimes from occurring.

C. Cybersecurity Training

A majority of people have answered either “no”, or “maybe” when questioned if they have received any cybersecurity education or training from their bank as a part and parcel of being that bank’s customer as shown in Fig.4.

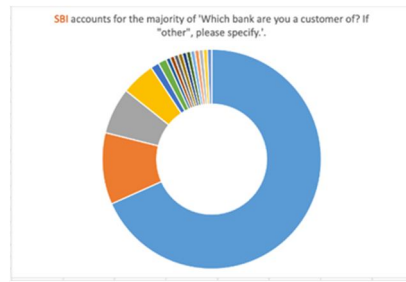


Fig.3 Customer information of Bank

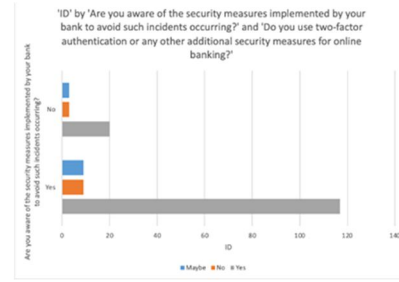


Fig.4 Cyber security awareness

D. Updating Passwords

According to McAfee, the American global computer security software company that specializes in antiviruses, one should ideally update their passwords every three months.

So, judging by the statistics, it is reassuring that about forty percent of people seasonally change their passwords, but the fact that about twenty-six percent never do, or do so on an annual basis cements a concern that people are either unaware of the cyber threats lurking at every corner of the internet (but especially the banking sector), or are uncaring of the same.

E. Additional Suggestions

As a way for people to give their two cents as a suggestion for banks on increasing trust among customers and solidifying their stance on cybersecurity and cybercrimes, one question in the survey was dedicated to the people to add their additional security measures or features that they would like to see implemented by banks to enhance cyber security.

Some of the answers included:

- Banking applications shouldn't open if VPN is in use.
- Use a jumbled keyboard for login or signup credentials.
- Enable facial recognition.
- Enable three-layered authentication, as opposed to two-factor authentication.
- "Provision of immediate solutions by making a consortium of all the public or private sector banks with dedicated arm/departments in all said banks, as it is easily traceable where the fraudster has deposited your money, but you cannot directly approach the bank immediately."
- Require regular reviews as hackers use different techniques
- Usage of biometric authentication.

As we can see, many of these ideas are already at play in a majority of banks used by customers, but some of them are new, and some are valid, if not controversial.

VI. CONCLUSION

Throughout the course of this study, we have seen people that have either fallen victim to, or stood against digital malpractice of information, finances, and data. One way to make sure such losses are mitigated and rectified is to not only adopt a large-scale net (so to speak) to make sure the heavy-duty data doesn't fall into the wrong hands, but also make sure there are measures set in place for financial institutions that provide it the seal of trustworthiness of their customer base. This may include transparency on data and how it is handled, any security breaches that occur, and holding responsibility in case things go awry.

The evolving landscape of cyber threats demands continuous adaptation and innovation in cybersecurity measures. Developing a network security infrastructure is essential. Building robust firewalls, IDS and IPS (or collectively, IDPS), and employing proper encryption protocols that are up to date and highly resistant to breaches are among the need of the hour. Additionally, we need to ensure the trustworthiness of the digital systems in the perspective of the customer, which is to say- providing information regarding how a customer's data is handled, stored and protected. Providing regular updates on security measures and taking accountability of breaches (if any) are surefire ways to build trust and to enhance the overall security of the system. This necessitates that banks remain agile and proactive in strengthening their cybersecurity posture[4].

Now, we can also put armour on to the customer. Financial institutions can also be advised or instructed to invest in educating both the customer and the employee about best use practices, including recognizing phishing attempts, knowing when and how to update software, and the importance of strong and confidential passwords.

Furthermore, the interconnected nature of the financial sector means that a cyber incident affecting one institution can have cascading effects on others (as mentioned just a couple lines prior), amplifying the potential impact on the entire financial ecosystem. As financial institutions increasingly rely on third-party vendors and service providers to enhance their offerings, the security of these partnerships becomes paramount. Collaborative efforts between banks, regulators, and industry stakeholders are crucial to establish common cybersecurity standards and best practices to fortify the resilience of the entire financial system.

Lastly, incident response and recovery are also good weapons to keep in the arsenal. Having them is crucial for financial institutes like banks to act swiftly, communicate transparently (as mentioned prior), and implement plans already in place for this exact situation and scenario. This not only aids in recovery but also provides a demonstration of the dedication towards customer and data protection.

An effective cybersecurity strategy requires a multi-layered approach, encompassing technological solutions, employee training, collaboration with industry peers and regulatory bodies, and constant vigilance to detect and respond to emerging threats. Only by adopting a proactive and comprehensive cybersecurity stance can banks build trust and resilience in the face of cyber challenges, ensuring the security and stability of the entire financial ecosystem.

REFERENCES

- [1] <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0>
- [2] <https://www.rbi.org.in/#>
- [3] https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/FR20Risk%20Based%20Supervision_draft%20v2.pdf
- [4] <https://www2.deloitte.com/us/en/insights/industry/financialservices/digitalization-in-banking.html>