International Journal of Education, Modern Management, Applied Science & Social Science (IJEMMASSS)
ISSN : 2581-9925, Impact Factor: 6.340, Volume 03, No. 03(I), July - September, 2021, pp.111-120

A STUDY TO ANALYSE THE IMPACT OF NEW RBI CYBER SECURITY GUIDELINES AND ITS COMPARISON WITH NIST FRAMEWORK

Dr. Nidhi Gupta*

ABSTRACT

Cyber security has become a growing concern for banks and financial institutions nowadays to protect data from unauthorized alterations and access. Cyber security has become a primary challenge to avoid huge financial losses. This is the reason cybercrime is receiving a huge amount of attention. Cyber security has become a major issue to national security in India. Most of the financial institutions and banks rely on technology for their operations. Sensitive data of banks can be at risk without proper cyber security measures taking place. It is important for banks and other financial institutions to know how cyber criminals operate and what are the latest security threats. Indian banking sector is highly vulnerable to cyber threats as they don't have any security technology that is considered reliable against the latest threats. However, building up cyber security in banks is not a one-time effort. Instead, it is an ongoing process. It is important to monitor the systems constantly through surveillance and identify common loopholes in security measures of financial transactions. It is important to constantly update and upgrade hardware and software to address the vulnerabilities in old versions. The banking sector in India has been through several major changes in its functioning and structure since 1991 when India has witnessed liberalization in its true form. India has welcomed a lot of foreign multinationals to enter its market and raised the competition significantly. Many customer-oriented strategies have come into practice. The rising dependence on information technology has also brought cyber security risks, especially in the banking industry. Reserve Bank of India (RBI) had sent a circular to all the Indian banks' CEOs named "Cyber Security Framework in Banks", stating that the banks should urgently place a robust resilience/cyber security framework for complete preparedness against online threats. On the other hand, the NIST cybersecurity framework provides a computer security guideline for private organizations to improve their preparedness to prevent, detect, and avoid cyber-attacks. This framework is used by many countries like Israel and Japan and has been translated to several foreign languages. In this study, we are going to compare NIST and RBI cyber security frameworks. In addition, we will understand common cyber security threats to e-banking in India and how RBI can help prevent them.

Keywords: *RBI Framework, NIST Framework, Cyber Security, Cyber Threats, Financial Institutions.*

Introduction

Indian banks have been aggressive in adopting latest and digital technologies to improve their revenues and customer base since 2010. Customers have also shifted their preference over digital platforms. However, it is observed that banks have been slow in adopting cutting-edge cyber security practices. There has been a paradigm shift in attacks using its behavior, source, attack vectors, and motives. Hence, it is a sign that age-old multilayered protection in the banks is not sufficient. Cyber security incidents are growing rapidly across the world and most of them are large-scale frauds and breaches. Along with severe financial loss, these breaches can affect the reputation of banks badly. This way, the Reserve Bank of India (RBI) has taken measures to protect the banks by strengthening their cyber security practices due to the highly sophisticated quantum and nature of attacks (pwc). Focus on digitization has been increased in Indian banks, especially with the wake of COVID-19. They have digitized both back-end and front-desk operations. Cyber attacks have been persistent in nature and attackers are constantly on the lookout for easy targets to initiate malicious attacks to steal sensitive data in banks. Banks depend highly on online and mobile banking but their security tends to be weak. Hence, cyber security risks are very common. Cybercriminals usually prefer customer and employee data from banks and leak the same for money (S.R., 2021). Cyber attacks have happened in various locations and business sectors. Some of the common examples are:

[G] Jagran College of Arts, Science and Commerce, Saket Nagar Kanpur Nagar, Uttar Pradesh, India.

- **Cosmos Bank, Pune:** In 2018, Pune-based Cosmos Bank suffered an attack where attackers hacked into the ATM server of the bank, stole all the card details, and drained off Rs. 94.42 crores and withdrew the amount quickly from 28 countries. Hence, authorized people must strengthen their security systems (S.R., 2021).

Fig. 1: A quick review of how it happened (Credit: The Economic Times)

- **Canara Bank ATM:** In 2018, hackers targeted Canara Bank ATM servers. They stole the ATM details of over 300 users and siphoned over Rs. 20 lakh from several accounts. They stole Rs. 20 Lakh using skimming devices on ATMs. This way, banks should enhance their ATMs' security features to avoid such incidents in future (S.R., 2021).

Fig. 2: A media report on Canara Bank ATM incident (Source: Times of India)

- **UIDAI:** One of the biggest data breaches in the world was reported in 2018 when Aadhar card details of 1.1 billion citizens were leaked in India. The Unique Identification Authority of India (UIDAI) had officially announced its data breach through notification and mentioning the hacking of over 210 websites by the Government of India. Hackers stole details like PAN, Aadhar number, IFSC codes of bank accounts linked with Aadhar, and other private data of the citizens. It was also observed that Aadhar information was being sold by anonymous sellers over WhatsApp for Rs. 500. Even worse, one could print out fake Aadhar cards for only Rs. 300 (S.R., 2021).
- **SIM Swap:** In August 2018, two Navi Mumbai-based hackers fraudulently collected SIM card details of customers and transferred around Rs. 4 crores from their bank accounts through online banking (S.R., 2021).

It is time for banks and the common public to take the above incidents as a wake-up call because cyber risks are still not over. Other organizations should also consider the following security threats and guidelines and implement them. One of the most ideal ways to control the risk of losing personal data to malicious actors is not sharing it to unknown people (S.R., 2021).

Common Security Threats

- **Anti-Fraud Bypass:** Considering the rise in digital transactions, cyber criminals are looking for the tricks to initiate large-scale anti-fraud bypass by imitating real fingerprints stolen from the device of someone else.
- **ATM Malware:** It is designed to hack ATMs to withdraw money illegally.
- **Phishing:** It is a very common method to trick users into clicking and accessing malicious links and installing malware on their devices. This way, they can steal login details and other user data.
- **Account-based Frauds:** It is another basic type of fraud which focuses mainly on hacking and stealing sensitive data like password, OTP, and account details.
- **Identity Theft:** Cybercriminals sell customers' data and get personal information without their consent and contact the people users know to borrow money.
- **Employee Threat:** Sometimes annoyed and dissatisfied staff breach the policies of their company and it leads to security threats.
- **Ransomware:** Small banks usually lack IT resources, cyber security protocols, and have obsolete security measures. These attacks are usually targeted at them. Hence, banks should have proper security measures in their networks to prevent such attacks.

What should Banks do to Prevent Cyber Threats?

- **Cloud Security:** Banks should assess their cloud security time to time to keep it updated. They should assess best practices, compliance structures, and existing state. Multifactor authentication is one of the best ways to protect cloud platforms. They should implement disaster management tools to protect against cyber threats and automate threat detection.
- **Keeping Employees Aware:** Banks should provide complete training to employees and prepare them against cyber threats.
- **Strict Access Control:** Access should be limited to employees who actually need it, rather than sharing the same with contractors, part-time staff etc. Strict access control policies must be implemented while allowing employees to access the information.
- **Disaster Recovery:** Banks and financial organizations must have robust alternate plans to secure their data, avoid data loss, and minimize downtime.
- **Encryption:** Cryptography is widely used to encrypt sensitive data.

The RBI has already warned about the rising cyber attacks in the banking sector during the lockdown period due to COVID-19. RBI has conducted systematic risk survey (SRS) in 2020 and found banks in 'high risk' category of cyber attacks. The RBI has issued over ten alerts in the recent Financial Security Report on several cyber threats and advisories on best security practices since March 2020. Indian Computer Emergency Response Team (CERT-In) is closely looking at some of the alerts and advisories. CERT-In is using different sources to analyze threat intelligence, tracking recent cyber risks, and issuing alerts and advisories on a regular basis (The Hindu, 2020).

In this day and age, organizations need to mitigate cyber security risks while fulfilling their needs. The National Institute of Standards and Technology (NIST) has developed a cyber security framework with its stakeholders to help businesses control their cyber security risks. Several organizations and communities worldwide have become the users of this framework.

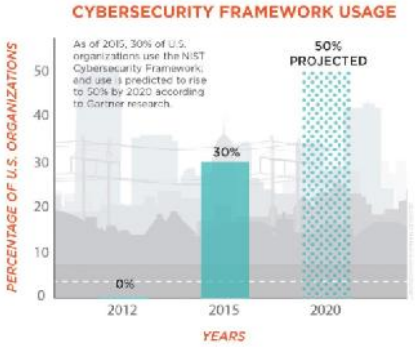

Fig. 3: Growth of NIST Framework User-base[1]

NIST Framework integrates best security practices and industry standards to mitigate cyber security risks in organizations. It enables all employees in an organization to develop a complete knowledge about online threats by providing a common ground to them at all points. NIST has coordinated with several government and private-sector experts to develop a framework. Along with helping to understand cyber threats, impacts, and vulnerabilities, the framework also makes organizations aware of the solutions to mitigate risks at their own levels. The framework has been designed to help organizations to recover from breaches and respond to those incidents. It prompts the organizations to detect the root causes and teaches them to improve. This framework has been embraced by several global leaders like Microsoft, JP Morgan Chase, Intel, Boeing, Ontario Energy Board, Nippon Telegraph, Bank of England, etc. All the domestic and international markets implement this framework.

Review of Literature

There is nothing much easier and more convenient than internet banking in this day and age. But cyber threats pose a significant challenge to e-commerce and internet banking. **Alghazo et al. (2017)** analyze cyber security in online banking in depth in three emerging economies and propose a novel study to cut down on cyber security risks to fill the gap between customers and banks. They proposed a model on the basis of survey results on digital banking in India, Pakistan, and Saudi Arabia. The survey is based on the internet banking practices of users. They analyzed the awareness of common internet banking risks and cyber security. The study suggests banks to incorporate a lot of services on their portal to reduce operational cost. Latest security technologies must be integrated to secure communication between customers and banks.

On the other hand, **Singh et al. (2020)** propose a framework of IT Governance for the banking industry in India. They researched the factors that can help predict customer faith in retail banking. They combined the legacy SERVQUAL model (which captures customer service insight with five dimensions, namely assurance, reliability, empathy, tangibles, and responsiveness, and three important cyber security factors (integrity, confidentiality, and availability) for the IT governance framework in the banking sector in India. The study suggests that consumers have less to moderate trust in the existing banking system in India and other aspects of its service quality. Hence, it can implement some important government policies which need integrity and confidentiality.

The 1990s was the era of liberalization on investments in India. Financial institutions have greatly played a vital role in Indian economy with significant improvements over the efficiency and quality of services. It is almost impossible to imagine the world without technology in this day and age, and so are the banks. However, they are under scrutiny when it comes to knowing what their customers need to excel in providing services. In addition, it is not easy to predict, treat, and detect cyber threats. **Pradeep (2015)** analyzes several banking services relying on technology, needs for cyber security, and regulation of IT in banking by showing the complexity of cyber crimes that took place in India from 2010 to 2013.

[1] https://www.nist.gov/industry-impacts/cybersecurity-framework

Cyber security consists of practices formed to protect data from authorized alterations and access. Unfortunately, cyber security risks are getting more attention than the potential of digitalization. Cyber security has become a matter of national security. Most of the operations in financial institutions or banks rely on technology, including the use of the internet. Sensitive data of banks could be at severe threat without proper cyber security measures. Banks are known to be highly vulnerable to cyber threats. No individual security technology can be sufficient for the IT systems of banks. **Manoj (2021)** analyses the approach of banks for controlling cyber security risks. The study suggests that cyber security in banks is not a one-time practice. Instead, it is an ongoing process. It is vital to monitor the systems constantly with surveillance technologies to keep track of loopholes. It is vital to keep the hardware and software up-to-date to address the vulnerabilities.

In this day and age of digitalization, cyber threats have put data and assets of institutions, corporations, people, and governments at stake, and so are the banks. It has become basic for banks to offer low-interest rates for sustainability. Fintech is a financial technology concept that has emerged as an advanced communication and transaction mechanism to meet the increasing demand for tailored financial portfolios. The collaboration between the banks and fintech organizations has been improved to provide better services to customers. This way, **Najaf et al. (2021)** argue that cyber security risk has been elevated with the alliance between Fintech and banking organizations. In addition, they come up with a theoretical framework to discuss several cyber threats. The study suggests that there could be a high cost and benefit of alliance in raising sustainability and profitability if both banks and fintech organizations abate cyber threats.

Data security is still a major challenge to deal with cyber threats because of lack of control and awareness. **Jidiga & Sammulal (2013)** conducted a brief survey on anomalies of cyber security in common applications and present ingredients of information present in this world. Hence, they focused on major malwares and malicious threats that were encountered over the past three years. A 3-LSP (3-Layer Security Paradigm) has been proposed that can match all technological aspects of potential areas. There is a multilevel security model in Layer-1 to spread awareness of the threats with common security ethics. This study proposes MEAM e-awareness model and 3-LSP model to help users control their security and choose how to avoid threats. They present only one security paradigm level on awareness in this paper because awareness is an important area to come up with a new type of ethical tools.

Research Objectives

- To understand common cyber threats used against banks in India
- To know the cyber security challenges in Indian banks
- To form a plan of action for cyber security in banks

Research Questions

- What Are The Cyber Security Threats And Challenges For E-banking In India and How new RBI Cyber Security Guidelines are going to protect Indian Banks?
- What is the comparison between NIST and RBI Framework, and how to strengthen the RBI Cyber Security Framework?

Methodology

Indian banks have gained over 80% of customers since the Government of India announced Jan Dhan Yojana for every Indian to open a bank account with zero balance (IndiaSpent, 2019). Hence, it becomes a matter of data security for billions of Indians who have accounts in various banks. Majority of Indians have a bank account owing to the government initiatives but concerns over online banking security are very low so far. Hence, we asked the respondents about security practices their banks follow for the security of banks' and customers' data. In order to answer and analyze the above research questions, this study relies on primary data. For the collection of information, we have framed a structured questionnaire which has been circulated among higher officials and employees in Indian banks. We conducted a survey through Google Forms and found responses from 200 participants. We consulted various research papers, banking reports (such as, Deolitte, RBI, McKinsey etc.), news links from NDTV, MoneyControl, Economic Times, Mint, etc. and other sources for secondary information.

Q1. Do you agree that RBI's latest cyber security guidelines help your bank to combat cyber threats?

Here, the majority of people (62.5%) have trust in RBI's recent cyber security guidelines, while the rest 37.5% are either neutral or disagree with the fact that these guidelines would do any help to their organization (Fig. 4).

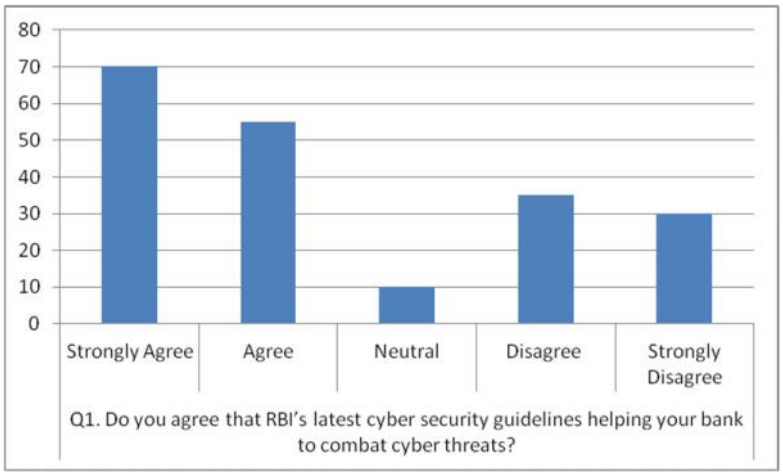

Fig. 4: Measuring Effectiveness of RBI Cyber Security Guidelines

Q2. Does your bank comply with the RBI cyber security framework?

Here, we found 100 employees and managerial staff (50%) who agree that their organizations do comply with RBI cyber security guidelines, while 85 (42.5%) don't agree, and the rest 15 (7.5%) people were not sure about that (Fig. 5).

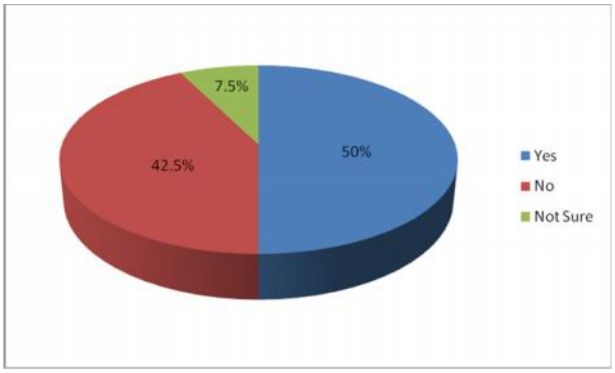

Fig. 5: Compliance of RBI Cyber Security Framework

Q3. Do you know about the NIST Framework?

This question was very important to determine the awareness about the NIST framework in Indian banks and common people. We asked 200 respondents out of which 37.5% of people knew about the NIST framework and only 12.5% of people had basic information about this framework, while the remaining 50% had no idea about NIST and its guidelines for organization (Fig. 6).

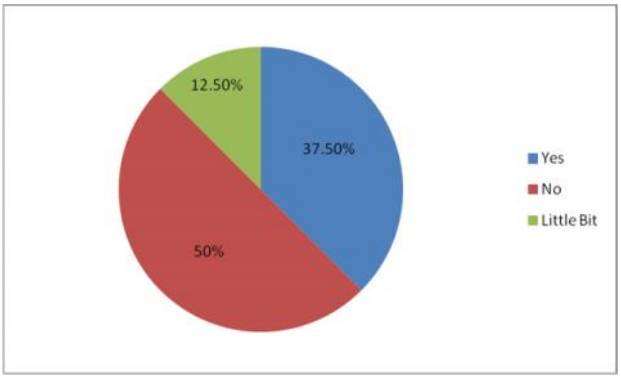

Fig. 6: Awareness about NIST Framework

Q4. Do you agree that the NIST framework would fit into Indian banks and enhance their security?

Here, the majority (37.5%) strongly agree that the NIST framework would comply with Indian banks and will help in improving their security as it has been successful in developed countries, while 12.5% agree with that. On the other side, the rest of 25% and 22.5% people disagree and strongly disagree with that question. So, we found mixed reactions when it comes to implementing the NIST framework in Indian banks (Fig. 7).

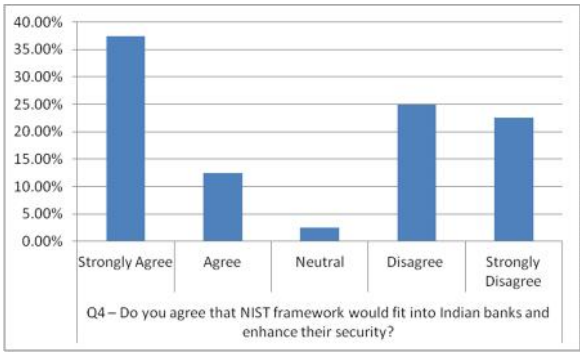

Fig. 7: NIST Framework Compliance with Indian Banks

Q5. When a critical cyber attack hits your bank, is your bank ready to deal with it?

This question gives an insight to how prepared our Indian banks are from latest security threats. In this study, 73% people believe that banks are prepared to deal with cyber attacks while the rest 16% and 11.5% were either negative or doubtful about preparedness of Indian banks if any security threat occurs (Fig. 8).

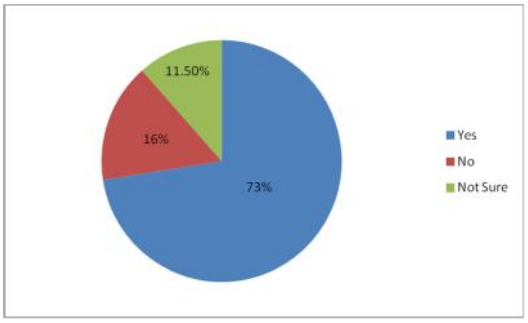

Fig. 8: Preparedness of Banks against Cyber Attacks

Q6. Do you believe that all small banks should work together against cyber attacks?

In this survey, we found 86% of people believe that all small banks should work collectively to prevent cyber attacks in our banking system (Fig. 9).

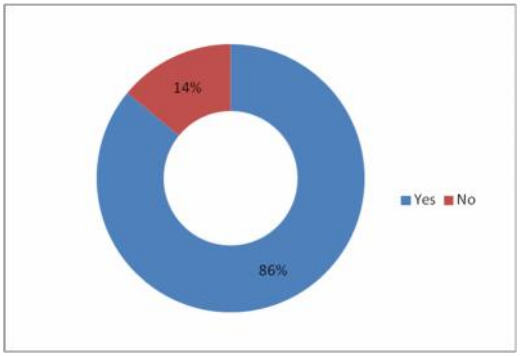

Fig. 9: Should Banks Work Together?

Q7. Are you educating your customers about best practices to prevent cyber threats and identity theft?

In our survey, we found that around 79% of employees suggest that their banks are educating their customers about best security practices and tips to prevent identity theft through SMS, email, and other means (Fig. 10).

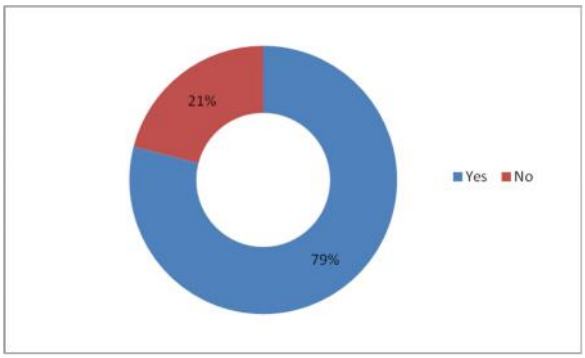

Fig. 10: Customers' Awareness about Cyber Threats

Results

In this study, it is observed that both banks and customers should take responsibility to protect their data against cyber attacks and use certain measures to prevent those threats. Cybercrime is constantly rising in India. According to a Symantec report, India is the third most common target of malicious activities, following the US and China. Considering the drastic rise in cyber crimes, the Reserve Bank of India has issued guidelines for all banks to implement a framework for cyber security. It prescribes the appropriate approach for concrete steps against cybercrime and frauds to protect customers' interest, ensure continuity of operations, and overcome financial losses (Clari5).

The Reserve Bank of India has made digital payment security stricter for improved compliance and control in banks and other regulated organizations. The occurrences of outages, security breaches, and frauds are rising in the thriving digital ecosystem in India. It is the right time for the RBI to set the directives and guidelines for online banking security. The RBI has issued guidelines for internet banking in commercial banks, mobile payments, payment banks, financial institutions, and non-banking lenders. This move might improve the security and convenience with digital payment channels. Those directives have guidelines for implementation, strong governance, and monitoring of some minimum standards on security controls for card payments, mobile and internet banking, etc. Service outages are the next major hurdle for the digital banking app of SBI, the largest lender in India. Hence, important guidelines have been provided by the "Master Direction" for regulated entities to establish common minimum security compliances and robust governance for digital payment services (Business Today, 2021).

Comparison between RBI and NIST Framework

RBI Framework	NIST Framework
Surveillance – Cyber attacks never come with warnings. Hence, RBI has recommended banks to ensure constant surveillance against cyber threats.	**Governance** – All the procedures, policies, and processes to keep track of legal risk, regulatory risk, operational, and environmental needs are managed by the procedures, policies, and processes of management and it is also reported of cyber security threats.
Customer Data – Banks collect customers' sensitive and personal data to deliver best digital services to meet their needs. RBI recommends banks to take proper steps to ensure uncompromised integrity, confidentiality and availability of data.	**Business Environment** – The stakeholders, objectives, and activities are prioritized and understood to inform cyber security responsibilities, roles, and risk management.
Reporting – Banks are also instructed to report against any unusual incident or activity to the RBI, even when such attempts have been failed.	**Risk Assessment and Management** – The organization keeps track of cyber threats to their operations like functions, image, mission, or reputation, individuals and assets. In addition, the priorities, limitations, risk assumptions and tolerance are established by the organization and used for taking risk management decisions.

Inventory Management – RBI also has a guideline for banks to manage their IT assets, such as business applications and infrastructure, IP addresses, domains, sub-domains, etc.	**Asset Management** – NIST has identified all the devices, data, personnel, facilities, and systems that help in meeting business goals and managed them well to meet their organizational goals and risk management.
Software updates – RBI instructs banks to maintain centralized, updated, inventory of authorized software.	
Configurations – RBI guides banks to apply and document basic security configurations of all devices.	Maintenance – Repairs and maintenance of information systems and industrial control components can be done with procedures and policies.
Vendor Risk Control – Banks are held liable for proper security risk management from partner and outsourcing arrangements.	Supply Chain Risk Management – The priorities, risk tolerances, priorities, and assumptions of an organization are used and established to help in risk decisions related to supply chain risk management. The processes have been established and implemented to determine, identify, and manage risks in the supply chain.
Real-time threat prevention – RBI guides banks to have a strong defense mechanism against spread, installation, and execution of malicious files at several points and implement secure gateways with deep scanning.	**Cybersecurity Awareness Training** – NIST puts emphasis on proper training and education for partners and personnel in an organization to handle their responsibilities and duties related to cyber security with their regular procedures, agreements, and policies.
Anti-phishing – Banks have been mandated to opt for anti-phishing services to detect and kill phishing/rogue apps and websites.	
Data Leak Prevention – Banks are required to have proper data leakage/loss prevention mechanisms to protect confidential and sensitive customer and business data.	**Data Security** – Organization's risk management strategy is used to manage records and information to protect the integrity, confidentiality, and availability of data.

Source: CloudSEK (2020) for RBI Guidelines and NIST Framework 1.1 (2018)[1]

Conclusion

With over 302 million users, India ranks second with the largest internet user base but Indian cyber space needs robust protection. Banking sector has been through a great IT revolution but it is highly vulnerable to security threats. Hence, a robust framework is still important to prevent recent cybersecurity risks like phishing, DDoS, fraudulent activities, malicious acts, and other risks. In this study, we have analyzed RBI and NIST cyber security frameworks to determine the best security practices for banks and financial institutions.

References

1. *Cyber Security in Banking*. pwc India. Retrieved 2 June 2021, from
2. https://www.pwc.in/consulting/cyber-security/banking.html.
3. S, R. (2021). *4 Biggest Cyber Security Threats for Indian Banking Sector*. GreatLearning Blog. Retrieved 2 June 2021, from https://www.mygreatlearning.com/blog/biggest-cyber-security-threats-indian-banking-sector/.
4. *Cyber threats against banking industry on the rise in post Covid-19 lockdown phase, says RBI*. The Hindu Business Line. (2020). Retrieved 2 June 2021, from https://www.thehindubusinessline.com/money-and-banking/cyber-threats-against-banking-industry-on-the-rise-in-post-covid-19-lockdown-phase-says-rbi/article32201404.ece.
5. NIST Framework. Retrieved from https://www.nist.gov/industry-impacts/cybersecurity-framework.
6. IndiaSpent. (2019). Record Number of Indians with Bank Accounts. So Why Is Financial Inclusion Low? Retrieved at https://www.indiaspend.com/record-number-of-indians-with-bank-accounts-so-why-is-financialinclusion-low-13223/
7. Alghazo, J. M., Kazmi, Z., & Latif, G. (2017). Cyber security analysis of internet banking in emerging countries: User and bank perspectives. In *2017 4th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS)* (pp. 1-6). IEEE.
8. Singh, R., Pandiya, B., Upadhyay, C. K., & Singh, M. K. (2020). IT-Governance Framework Considering Service Quality and Information Security in Banks in India. *International Journal of Human Capital and Information Technology Professionals (IJHCITP)*, *11*(1), 64-91.

[1] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

9. Pradeep, M. D. (2015). Impact of Information Technology in Banking-Cyber Law and Cyber Security in India. *International Journal of Management, IT & Engineering*, *5*(7), 2249-0558.
10. Manoj, K. (2021). Banks' Holistic Approach to Cyber Security: Tools to Mitigate Cyber Risk. *International Journal of Advanced Research in Engineering and Technology (IJARET)*, *12*(1), 902-910. https://doi.org/10.34218/IJARET.12.1.2021.082.
11. Najaf, K., Mostafiz, M. I., & Najaf, R. (2021). Fintech firms and banks sustainability: Why cybersecurity risk matters?. *International Journal of Financial Engineering*, 2150019.
12. Clari5. How can RBI's latest guidelines help Indian banks combat cybercrime?. Available at https://www.clari5.com/multichannel-banking-technology/can-rbis-latest-guidelines-help-indian-banks-combat-cybercrime/
13. Business Today (2021). RBI tightens digital payment security norms for lenders; issues new rules. Retrieved 13 June 2021, from https://www.businesstoday.in/sectors/banks/rbi-tightens-digital-payment-security-norms-for-lenders-issues-new-rules/story/431755.html
14. RBI guidelines for banks to combat escalating cyber attacks - CloudSEK. (2020). Retrieved 13 June 2021, from https://cloudsek.com/rbi-guidelines-on-how-banks-can-be-resilient-in-the-face-of-escalating-cyber-attacks/

Appendix A

Q1. Do you agree that RBI's latest cyber security guidelines help your bank to combat cyber threats?
- Strongly Disagree
- Disagree
- Neither Agree nor Disagree
- Agree
- Strongly Agree

Q2. Does your bank comply with the RBI cybersecurity framework?
- Yes
- No
- Not Sure

Q3. Do you know about the NIST framework?
- Yes
- No
- Little bit

Q4. Do you agree that the NIST framework would fit into Indian banks and enhance their security?
- Strongly Disagree
- Disagree
- Neither Agree nor Disagree
- Agree
- Strongly Agree

Q5. When a critical cyber attack hits your bank, is your bank ready to deal with it?
- Yes
- No
- Not Sure

Q6. Do you believe that there is a strong need to have stricter standards for retailers to ensure higher security?
- Definitely Yes
- No, it could affect their freedom of doing business

Q7. Do you believe that all small banks should work together against cyber attacks?
- Yes
- No

Q8. What kind of data security strategy does your bank have?
- IT Risk Management
- Disaster Management and Resilience
- Trained Staff to work against cyber threats
- Investigate potential breaches time to time

Q9. Are you doing a complete risk assessment to protect valuable customers' data?
- Yes
- No

Q10. Are you educating your customers about best practices to prevent cyber threats and identity theft?
- Yes
- No.

❖◆❖