WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Strengthening Banking Security in India: Advanced Approaches to Combat Hacking and Cyber Threats

Alphina jose

Kristu Jayanti College (Autonomous), Department of Commerce (PG), Bangalore, Karnataka
alphinathomasjose@gmail.com
DOI : https://doi.org/10.55248/gengpi.6.0325.11132

A B S T R A C T

This study investigated cybersecurity perceptions and practices within Indian banking sector, focusing on the interconnectedness of the key factors and the influence of demographic variables. Utilizing survey data from 62 respondents, the research revealed a consistent perception of cybersecurity vulnerabilities, with respondents expressing concerns about the effectiveness of current measures. Spearman's rho correlation analysis highlighted strong interrelationships between factors such as employee training, regulatory guidance, resource allocation, and leadership commitment, underscoring the necessity of a holistic cybersecurity approach. Kruskal-Wallis tests indicated that age did not significantly influence these perceptions, suggesting a broadly shared concerns across the sector. the study's findings have practical implications for banking institutions and policymakers seeking to enhance cybersecurity resilience in the Indian financial sector, underscoring the importance of collaborative efforts between banks, regulatory bodies, and technology providers, as well as strategic investments in advanced technologies and continuous training to mitigate evolving cyber threats and maintain the integrity and stability of the financial system.

Keywords: Cyber securities, Indian banking sector, regulatory bodies, financial sector

INTRODUCTION

India, a nation of over 1.4 billion people, is rapidly transforming and experiencing a fast growth in its economy. India, being a rapidly developing economy where in its banking sector has played a key role, driven by the factors such as financial inclusion, rising incomes, and the proliferation of digital technologies. However, this growth has also been accompanied by a surge in cyber threats, including hacking, phishing, and malware attacks. These threats have brought in a significant risk to the security and stability of the Indian banking system, as well as the financial well- being of the individuals and businesses.

Though the technological advancements have transformed the way the financial services are delivered, with enhanced accessibility and convenience for customers, they have also exposed the sector to an increasing array of cyber threats, and this has created, data breaches, financial fraud, have become pervasive challenges, threatening the integrity, privacy, and security of banking operations. These risks have amplified due to the increased reliance on digital platforms for banking transactions, mobile payments, and online services. The need to safeguard sensitive financial data, maintain the trust of millions of users, and protect the country's financial ecosystem has never been more critical. As the cybercriminals continuously evolve their tactics, the existing security frameworks within Indian banks need to be enhanced to counter sophisticated attacks effectively.

The main of this research is to explore the challenges faced by the Indian banking sector in securing digital transactions and sensitive customer data. This paper will examine the various cyber threats that is actually faced in the Indian banking sector and discuss the advanced approaches that can be taken to combat them.

REVIEW OF LITERATURE

1. Enhancing cybersecurity resilience in Indian banking: Challenges and strategies: by DR. Pawan Kumar Maurya, assistant professor, department of commerce, Pt. DDU Govt. PG. College, Rajaji Puram, Lucknow 2023

The banking industry in India, crucial to the country's economic growth and stability, is experiencing a radical digital revolution, ushering in a new era of customer-friendly service. However, several new cybersecurity challenges have emerged as a result of this shift. This study digs into the core areas of cybersecurity in Indian banking, with a primary focus on identifying the primary difficulties, evaluating the solutions in place, and providing recommendations to strengthen the cybersecurity resilience of the sector. In the context of Indian banking, the importance of cybersecurity cannot be emphasized. Beyond just keeping money safe, it also ensures that personal information is kept private. Cybercriminals are drawn to the industry because of the volume of valuable financial data it stores. There is a great deal riding on customers' ability to trust digital transactions while using

financial services. The study aims to shed light on the most pressing issues in banking sector cybersecurity in India. Constant attention is required due to the ever-changing nature of cyber threats. Indian banks have taken a number of proactive measures in response to these threats. The article finishes with some suggestions for strengthening Indian financial institutions' resistance to cyberattacks. The suggestions include doing things like updating old systems, creating a mindset that values cybersecurity, using strong encryption for data, joining joint efforts, and educating the public. The study highlights the essential role of Indian banks in maintaining financial assets, consumer trust, and data integrity. Increasing cybersecurity resilience is an ongoing process that calls for constant teamwork, attention, and dedication to safety in this digital age marked by a constantly shifting cyber threat scenario.

2. Cyber security in Indian banking sector: by Nuruddin Khan & Sandeep Bala, research scholar, department of law, lovely professional university, Punjab, India, assistant professor, department of law, Asmita college of law, Mumbai 2021

Since 2010, Banks in India have quickly embraced fresher advancements and digital channels, with the fundamental target of expanding footprints and revenues. We have additionally seen client inclinations shift towards digital platforms. There is a perception, however, that the reception advanced cyber security practices have not stayed up with the pace of development of center business-empowering innovation. While in contrast with a few different areas, banks are certainly seen to be more proactive in contributing and further developing security practice, such measures might in any case be lacking thinking about the difficulties with the conventional way to deal with IT security. A change in perspective has as of late been seen in assaults taking advantage of the source, conduct, thought processes and vectors. This shows that the customary diverse safeguard that banks as of now have isn't sufficient. Globally, there is an in cyber security incidents and a few of them have been enormous scope breaks, cheats and heists. The effect of such breaks doesn't end with genuine monetary misfortune at the same time, much of the time, can likewise conceivably dissolve significant brand esteem. RBI has made a stride the correct way by understanding the innate requirement for banks to fortify their network safety act in the wake of the undeniably complex nature and quantum of assaults.

3. A critical evaluation of the challenges in cybersecurity of Indian banking and the possible ways to mitigate them: by Dr. Dinesh Pratap Singh, department of business administration, Bareilly college, Bareilly, mahatma Jyotiba Phule, Rohilkhand university, Bareilly, Uttar Pradesh, India 2022

Cybersecurity has emerged as a critical concern for the Indian banking sector, given the rapid adoption of digital technologies and the increasing sophistication of cyber threats. This study critically evaluates the challenges faced by Indian banks in maintaining robust cybersecurity measures, such as phishing attacks, malware, ransomware, data breaches, and insider threats. The research explores the key vulnerabilities within the sector, including legacy systems, inadequate cybersecurity frameworks, lack of skilled personnel, and regulatory challenges. Furthermore, it highlights possible mitigation strategies, such as enhancing cybersecurity infrastructure, adopting advanced technologies like artificial intelligence and blockchain, improving regulatory compliance, and promoting a culture of cybersecurity awareness among stakeholders. The study aims to provide actionable insights to strengthen the cybersecurity posture of Indian banks, thereby ensuring the safety and integrity of the banking ecosystem.

4. A study to analyze the impact of new RBI cyber security guidelines and its comparison with NIST framework: by Dr. Nidhi Gupta 2021

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.

5. Literature review on cybercrimes and its prevention mechanisms: by Annamalai Lakshmanan, national advanced IPv6 center, university sains Malaysia, Penang, Malaysia 2019

Cybercrimes is defined as the criminal activities carried out by means of using digital devices like computers through internet. Basically, a crime committed by using the internet is called as a cyber-crime. Now a day’s, information is wealth and also to earn money in an illegal way, cyber-attacks are happening, and data is been stolen from the servers or money is been stolen in an illegal way. So, this paper describes the list of cyber threats

happened around the world until now and its prevention mechanisms. Also, the cyber threats predictions in the upcoming year are also discussed in the final section and cyber threat analysis for January 2019 is also been discussed.

RESEARCH METHODOLOGY

The research aims to investigate the evolving landscapes of cyber threats facing Indian banks and evaluate the effectiveness of the advanced security approaches. To achieve this objective the study adopts questioner method that could be used to identify the reliable answer from banking experts, customers, and other users. Both primary data is collected through questioners and the secondary data is collected from other articles and other journals to find out more insight on the topic.

Though the study might seem to provide rich details, it is just limited in its generalizability to the entire Indian banking sector. The study concentrates on publicly reported cyberattacks and may not capture the full extent of the cyber threats faced by Indian banks, as many incidents may go unreported due to reputational concerns. And due to time constrain the research may not reflect the most recent development in the cyber threats and many security measures. And due to limited resources available, the research might not cover everything.

RESEACH OBJECTIVES

1. To identify and analyses the most prevalent cyber threats targeting Indian banks, focusing on phishing, malware, and ransomware attacks.
2. To evaluate the effectiveness of current cybersecurity measures employed by the Indian banks in mitigation these threats.
3. To explore the potential of artificial intelligence and machine learning in enhancing cybersecurity detection and prevention capabilities in the Indian banking sector.
4. To develop a set of practices recommendations for Indian banks to strengthen their cybersecurity defense against evolving cyber threats.

SAMPLING DESIGN

This study adopted a non-probability convenience sampling method, selecting respondents based on accessibility and willingness to participate.

SAMPLING APPROACH

The questionnaire was distributed through online platforms and direct communication, allowing for a broader reach and approach.

- The sample includes students, bank experts and other individuals who are aware of the banking securities.

SAMPLE SIZE

62 respondents participated in the study, ensuring sufficient data for statistical analysis.

This sampling approach ensures that the research findings are relevant and applicable.

STASTICAL TOOLS USED FOR DATA ANALYSIS

To analyze the collected data, SPSS was used to perform various statistical tests. These following are the different tools applied:

STATISTICAL TEST	**PURPOSE**
Descriptive statistics	To give out a solid understanding of the base data, before any tests are performed.
Reliability analysis (Cronbach's Alpha)	To prove the reliability of the survey data
One-sample Kolmogorov -Smirnov Test	To confirm the choice of statistical method on why non-parametric test was used.
Kruskal- Wallis H Test	To address whether age influenced the responses.
Correlations (Spearmen's Rho)	Presents the findings that explores the relationship between the Likert scale variables, that is by exploring the relationship between the different questions, this is the most important test used in this research.

The application of these statistics serves to rigorously analyze survey data, ensuring its validity and revealing meaningful relationships: descriptive statistics provide an overview of response patterns, reliability analysis confirms the consistency of the survey instrument, the K-S test justifies the use

of non- parametric methods due to data non-normality, Kruskal-Wallis tests for difference across demographic groups, and spearman's rho correlations uncover associations between cybersecurity perceptions, ultimately providing evidence- based insights to address research objectives related to strengthening banking security.

RESULTS AND DISCUSSIONS

Descriptive statistics

TABLE 1- DESCRIPTIVE STATISTICS DATA

Statistics

	N					
	Valid	Missing	Mean	Median	Mode	Std. Deviation
"I am confident that my bank has a comprehensive understanding of the current cyber threat landscape targeting the Indian banking sector."	62	0	2.35	2.50	1	1.307
"My bank effectively identifies and prioritizes emerging cyber threats based on their potential impact."	62	0	2.03	1.00	1	1.267
"My bank's incident response plan adequately addresses the evolving tactics of cybercriminals."	62	0	2.00	2.00	1	1.086
"The current security measures implemented by my bank are sufficient to protect against the majority of cyber threats."	62	0	2.23	2.00	1	1.247
"My bank's security audit processes effectively identify vulnerabilities in our systems."	62	0	2.16	2.00	1	1.217
"The level of cybersecurity training provided to employees at my bank is adequate for their roles."	62	0	2.45	3.00	1[a]	1.224
"The current regulatory framework provides sufficient guidance for cybersecurity in the banking field."	62	0	2.18	2.00	1	1.195
"My bank is actively exploring the potential of artificial intelligence (AI) and machine learning (ML) for cybersecurity."	62	0	2.31	3.00	3	1.095
"I believe that implementing threat intelligence platforms would significantly enhance my bank's cybersecurity posture."	62	0	2.21	2.00	1	1.307
"My bank is prepared to adopt blockchain technology to improve data security and transparency."	62	0	2.40	3.00	3	1.137
"My bank has a clear plan for implementing advanced security technologies."	62	0	2.19	2.00	1	1.157

"My bank effectively communicates cybersecurity best practices to its employees."	62	0	2.26	2.00	1	1.254
"I believe that increased collaboration and information sharing among banks would strengthen the overall cybersecurity of the sector."	62	0	2.23	2.00	1	1.220
"My bank has sufficient resources dedicated to cybersecurity incident response."	62	0	2.02	2.00	1	1.166
"The leadership within my bank prioritizes cybersecurity as a critical business function."	62	0	2.35	3.00	1[a]	1.161

a. Multiple modes exist. The smallest value is shown

The above table presents the descriptive analysis of 15 Likert scale items, revealing a consistent trend between 'disagree' and 'neutral' responses among the 62 respondents. Notably, the median value, which serves as the most reliable indicator of the central tendency for ordinal data, predominantly ranged from 2.00 to 3.00. this suggest a general perception that current cybersecurity measures and practices within Indian banks are not considered sufficiently robust, specially, respondents expressed disagreement regarding the understanding of cyber threats, the effectiveness of current security measures, and the adequacy of cybersecurity practices such as training, communication, and resource allocation. While there was some uncertainty regarding advanced technologies like AI/ML and blockchain, as indicated by neutral medians, the overall sentiment points to a need for significant improvement in cybersecurity strategies, the moderate variability in responses, reflected in the standard deviation, indicates that while a general trend foe subsequent inferential analyses and underscore the importance of addressing the identified weakness to strengthen cybersecurity within the Indian banking sector.

Reliability analysis (Cronbach's Alpha)

TABLE 2- RELIABILITY ANALYSIS DATA

Cronbach's Alpha	N of Items
0.837	15

The reliability of the 15item scale was assessed using Cronbach's Alpha, a measure of internal consistency. The analysis yielded a Cronbach's Alpha coefficient of 0.837, this value indicates a high level of internal consistency among the item, suggesting that they are reliably measuring the same underlying construct. Such a strong alpha value demonstrated that the items within the scale are closely related and consistently reflect the intended concept, thereby bolstering the confidence in the scale's reliability for further analysis and interpretation.

One-sample Kolmogorov- Smirnov Test

TABLE 3- One-sample Kolmogorov- Smirnov Test

One-Sample Kolmogorov-Smirnov Test								
	N			Most Extreme Differences			Test Statistic	Asymp. Sig. (2-tailed)
				Absolute	Positive	Negative		
"I am confident that my bank has a comprehensive understanding of the current cyber threat landscape targeting the Indian banking sector."	62	2.35	1.307	0.286	0.286	-0.189	0.286	.000[c]
"My bank effectively identifies and prioritizes emerging cyber threats based	62	2.03	1.267	0.373	0.373	-0.208	0.373	.000[c]

on their potential impact."								
"My bank's incident response plan adequately addresses the evolving tactics of cybercriminals."	62	2.00	1.086	0.305	0.305	-0.208	0.305	.000[c]
"The current security measures implemented by my bank are sufficient to protect against the majority of cyber threats."	62	2.23	1.247	0.289	0.289	-0.184	0.289	.000[c]
"My bank's security audit processes effectively identify vulnerabilities in our systems."	62	2.16	1.217	0.298	0.298	-0.206	0.298	.000[c]
"The level of cybersecurity training provided to employees at my bank is adequate for their roles."	62	2.45	1.224	0.221	0.221	-0.221	0.221	.000[c]
"The current regulatory framework provides sufficient guidance for cybersecurity in the banking field."	62	2.18	1.195	0.306	0.306	-0.238	0.306	.000[c]
"My bank is actively exploring the potential of artificial intelligence (AI) and machine learning (ML) for cybersecurity."	62	2.31	1.095	0.269	0.238	-0.269	0.269	.000[c]
"I believe that implementing threat intelligence platforms would significantly enhance my bank's cybersecurity posture."	62	2.21	1.307	0.306	0.306	-0.179	0.306	.000[c]
"My bank is prepared to adopt blockchain technology to improve data security and transparency."	62	2.40	1.137	0.248	0.214	-0.248	0.248	.000[c]
"My bank has a clear plan for implementing advanced security technologies."	62	2.19	1.157	0.252	0.252	-0.193	0.252	.000[c]
"My bank effectively communicates cybersecurity best practices to its employees."	62	2.26	1.254	0.278	0.278	-0.191	0.278	.000[c]
"I believe that increased collaboration and information sharing among banks would strengthen the overall cybersecurity of the sector."	62	2.23	1.220	0.294	0.294	-0.221	0.294	.000[c]
"My bank has sufficient	62	2.02	1.166	0.292	0.292	-0.192	0.292	.000[c]

resources dedicated to cybersecurity incident response."								
"The leadership within my bank prioritizes cybersecurity as a critical business function."	62	2.35	1.161	0.259	0.249	-0.259	0.259	.000[c]

The above test was conducted to evaluate the assumptions of normality for each of the 15 Likert scale items. The results demonstrate a statistically significant deviation from normality for all items, as evidenced by p-values of .000 ($p<.001$). this consistent findings across all the variables confirms that the data does not adhere to a normal distribution, a common characteristics of ordinal Likert scale data. Consequently, the use of non-parametric statistical methods, such as Spearman's rho correlation and the Kruskal-Wallis H test, was deemed appropriate for subsequent analyses, ensuring the robustness and validity of the statistical inferences drawn from this data set.

Kruskal-Wallis H Test

TABLE 4- Kruskal-Wallis H Test

Test Statistics			
	Kruskal-Wallis H	df	Asymp. Sig.
"I am confident that my bank has a comprehensive understanding of the current cyber threat landscape targeting the Indian banking sector."	0.651	3	0.885
"My bank effectively identifies and prioritizes emerging cyber threats based on their potential impact."	1.612	3	0.657
"My bank's incident response plan adequately addresses the evolving tactics of cybercriminals."	2.776	3	0.427
"The current security measures implemented by my bank are sufficient to protect against the majority of cyber threats."	2.462	3	0.482
"My bank's security audit processes effectively identify vulnerabilities in our systems."	0.711	3	0.871
"The level of cybersecurity training provided to employees at my bank is adequate for their roles."	3.616	3	0.306
"The current regulatory framework provides sufficient guidance for cybersecurity in the banking field."	2.722	3	0.436
"My bank is actively exploring the potential of artificial intelligence (AI) and machine learning (ML) for cybersecurity."	3.113	3	0.375
"I believe that implementing threat intelligence platforms would significantly enhance my bank's cybersecurity posture."	2.127	3	0.547
"My bank is prepared to adopt blockchain technology to improve data security and transparency."	2.167	3	0.539
"My bank has a clear plan for implementing advanced security technologies."	3.371	3	0.338
"My bank effectively communicates cybersecurity best practices to its employees."	3.027	3	0.388
"I believe that increased collaboration and information sharing among banks would strengthen the overall cybersecurity of the sector."	3.908	3	0.272
"My bank has sufficient resources dedicated to cybersecurity incident response."	2.376	3	0.498
"The leadership within my bank prioritizes cybersecurity as a critical business function."	1.557	3	0.669

The Kruskal-Wallis H test that's employed above shows whether any significant differences existed in respondents' perceptions, as measured by the 15 Likert scale items, across four distinct age groups, the analysis revealed that for all 15 questions, the resulting p-values were greater than the conventional significance level of 0.05. specifically, the Asymptotic significance values, ranging from 0.272 to 0.885, indicate that no statistically significant differences in responses were observed across the age categories. This suggests that respondents' perceptions regarding cybersecurity practices within the Indian banking sector, as captured by the survey, were not significantly influenced by their age. In essence, the data suggests a consistent perspective on cybersecurity issues across the age spectrum of the participants, indicating that age is not a distinguishing factor in shaping these views.

Correlations (Spearman's Rho)

TABLE 5- Correlations (Spearman's Rho)

Variable 1	**Variable 2**	**Correlation Value (Spearman's rho)**	**Significance Level**
Confidence in Cyber Threat Understanding	Threat Identification & Prioritization	0.306	* (0.05 level)
Confidence in Cyber Threat Understanding	Regulatory Guidance Adequacy	0.302	* (0.05 level)
Confidence in Cyber Threat Understanding	Threat Intelligence Platforms	0.348	** (0.01 level)
Confidence in Cyber Threat Understanding	Incident Response Resources	0.315	* (0.05 level)
Threat Identification & Prioritization	Incident Response Plan Adequacy	0.292	* (0.05 level)
Threat Identification & Prioritization	Regulatory Guidance Adequacy	0.267	* (0.05 level)
Threat Identification & Prioritization	Blockchain Adoption for Security	0.276	* (0.05 level)
Threat Identification & Prioritization	Collaboration Among Banks	0.376	** (0.01 level)
Threat Identification & Prioritization	Incident Response Resources	0.3	* (0.05 level)
Incident Response Plan Adequacy	Security Audit Effectiveness	0.378	** (0.01 level)
Incident Response Plan Adequacy	AI & ML for Cybersecurity	0.478	** (0.01 level)
Incident Response Plan Adequacy	Blockchain Adoption for Security	0.287	* (0.05 level)
Incident Response Plan Adequacy	Collaboration Among Banks	0.347	** (0.01 level)
Incident Response Plan Adequacy	Leadership Cybersecurity Priority	0.264	* (0.05 level)
Security Measures Effectiveness	Security Audit Effectiveness	0.339	** (0.01 level)
Security Measures Effectiveness	Employee Cybersecurity Training	0.368	** (0.01 level)
Security Measures Effectiveness	Regulatory Guidance Adequacy	0.424	** (0.01 level)
Security Measures Effectiveness	Collaboration Among Banks	0.278	* (0.05 level)
Security Measures Effectiveness	Incident Response Resources	0.31	* (0.05 level)

Security Measures Effectiveness	Leadership Cybersecurity Priority	0.359	** (0.01 level)
Security Audit Effectiveness	Employee Cybersecurity Training	0.195	* (0.05 level)
Security Audit Effectiveness	Regulatory Guidance Adequacy	0.307	* (0.05 level)
Security Audit Effectiveness	Blockchain Adoption for Security	0.261	* (0.05 level)
Security Audit Effectiveness	Incident Response Resources	0.262	* (0.05 level)
Security Audit Effectiveness	Leadership Cybersecurity Priority	0.451	** (0.01 level)
Employee Cybersecurity Training	Regulatory Guidance Adequacy	0.49	** (0.01 level)
Employee Cybersecurity Training	Threat Intelligence Platforms	0.352	** (0.01 level)
Employee Cybersecurity Training	Blockchain Adoption for Security	0.286	* (0.05 level)
Employee Cybersecurity Training	Advanced Security Technologies Plan	0.286	* (0.05 level)
Employee Cybersecurity Training	Collaboration Among Banks	0.402	** (0.01 level)
Employee Cybersecurity Training	Incident Response Resources	0.506	** (0.01 level)
Employee Cybersecurity Training	Leadership Cybersecurity Priority	0.378	** (0.01 level)
Regulatory Guidance Adequacy	AI & ML for Cybersecurity	0.371	** (0.01 level)
Regulatory Guidance Adequacy	Threat Intelligence Platforms	0.304	* (0.05 level)
Regulatory Guidance Adequacy	Advanced Security Technologies Plan	0.348	** (0.01 level)
Regulatory Guidance Adequacy	Collaboration Among Banks	0.49	** (0.01 level)
Regulatory Guidance Adequacy	Incident Response Resources	0.458	** (0.01 level)
Regulatory Guidance Adequacy	Leadership Cybersecurity Priority	0.417	** (0.01 level)
AI & ML for Cybersecurity	Threat Intelligence Platforms	0.3	* (0.05 level)
AI & ML for Cybersecurity	Blockchain Adoption for Security	0.35	** (0.01 level)
AI & ML for Cybersecurity	Advanced Security Technologies Plan	0.324	* (0.05 level)
AI & ML for Cybersecurity	Cybersecurity Best Practices Communication	0.437	** (0.01 level)
AI & ML for Cybersecurity	Incident Response Resources	0.31	* (0.05 level)
Threat Intelligence Platforms	Advanced Security Technologies Plan	0.323	* (0.05 level)
Threat Intelligence Platforms	Cybersecurity Best Practices Communication	0.325	** (0.01 level)

Threat Intelligence Platforms	Collaboration Among Banks	0.405	** (0.01 level)
Threat Intelligence Platforms	Incident Response Resources	0.309	* (0.05 level)
Advanced Security Technologies Plan	Cybersecurity Best Practices Communication	0.384	** (0.01 level)
Advanced Security Technologies Plan	Collaboration Among Banks	0.343	** (0.01 level)
Advanced Security Technologies Plan	Incident Response Resources	0.39	** (0.01 level)
Advanced Security Technologies Plan	Leadership Cybersecurity Priority	0.403	** (0.01 level)
Collaboration Among Banks	Incident Response Resources	0.42	** (0.01 level)
Collaboration Among Banks	Leadership Cybersecurity Priority	0.301	* (0.05 level)
Incident Response Resources	Leadership Cybersecurity Priority	0.384	** (0.01 level)

The correlation analysis revealed significant relationships between cybersecurity factors. Strong positive correlations were found between perceived understanding of cyber threats and effective threat management, regulatory adequacy, threat intelligence use, and resource availability, effective incident response plans were linked to strong audit AI/ML adoption, collaboration, and leadership support. Security measure effectiveness correlated strongly with audit, training, regulatory guidance, collaboration, resources, and leadership. Employee training showed strong ties to regulatory compliance, advanced technology use, collaboration, and resource availability. Overall, the findings highlights that a hostile approach, emphasizing training, collaboration, robust security measures, and strong leadership, is essential for strengthening cybersecurity in the Indian banking sector.

FINDINGS

1) **PERCEIVED CYBERSECUITY WEAKNESS**:

- Respondents generally expressed disagreement or neutrality regarding the effectiveness of current cybersecurity measures and practices within their banks.
- This includes perceived weaknesses and practices within their banks.

2) INTERCONNECTEDNESS OF CYBERSECURITY FACTORS:

- Significant positive correlations were found between various cybersecurity aspects, indicating that they are closely interrelated.
- Strong relationships between:
- Employee cybersecurity training and regulatory guidance, resource allocation, and leadership commitment.
- Effective security measures and robust security audits, adequate training, and regulatory satisfying.
- AI/ML adoption and strong incident response plans, regulatory guidance, and communication of the best practices.
- Collaboration among banks and regulatory guidance, incident response resources, and leadership commitment.

3) IMPORTANCE OF LEADERSHIP AND RESOURCES:

- Leadership prioritization of cybersecurity was strongly correlated with the availability of sufficient incident response resource.
- This highlights the crucial role of leadership in allocating resources for cybersecurity.
- AGE AS A NON-SIGNIFICANT FACTOR:
- Kruskal-Wallis H tests revealed no statistically significant differences in responses across age groups, suggesting that perceptions about cybersecurity are consistent across different age ranges.

4) DATA NON-NORMALITY:

- Kolmogorov-Smirnov tests confirmed that the Likert scale data was not normally distributed, justifying the use of non-parametric statistical methods.

5) HIGH SURVEY RELIABILITY:

- The Cronbach's Alpha test showed a high level of reliability within the survey.

6) MEDIAN RESPONSE TRENDS:

- The median values of the Likert scale responses leaned towards "Disagree" or "Neutral" on most of the questions relating to the current cyber security practices.

7) OVERALL IMPLICATIONS:

- The research underscores the need for a holistic approach to cybersecurity in the Indian banking sector, encompassing robust threats management, effective incident response, technological innovation, collaborative strategies, and strong leadership commitment.
- Emphasis should be placed on improving employee training, strengthening security audits, and ensuring adequate resource allocation.
- The findings suggest that collaboration and information sharing among banks can significantly enhance the overall cybersecurity posture of the sector.

CONCLUSION

This study investigated cybersecurity perceptions within the Indian banking sector, revealing a consistent sentiment that current measures require significant enhancement. The research highlighted the strong interdependence of key factors, notably employee training, leadership commitment, and resource availability, in establishing effective cybersecurity defenses. The research also found that age had no significant impact on these perceptions, indicating a broadly shared concern across the sector. The data reinforces the necessity of a comprehensive strategy that prioritizes robust training initiatives, fosters collaborative partnerships, and ensures decisive leadership. By focusing on these critical elements, Indian banks can strengthen their resilience against the ever-evolving landscapes of cyber threats, safeguarding the integrity and stability of the financial system.

REFERENSES

https://www.rbi.org.in/ - RBI publications

https://www.cert-in.org.in/ - CERT-In (Indian computer emergency response team)

https://cybercrime.gov.in/ - national cyber reporting portal

https://www2.deloitte.com/in/en/pages/financial-services/articles/in-fs-cybersecurity-in-the-indian-banking-industry.html - Cybersecurity in Indian banking industry by Deloitte.

https://www.esecurityplanet.com/cloud/cyber-security-in-banking/ - eSecurity planet

https://www.researchgate.net/publication/367968136_An_Overview_of_Cyber_Security_in_Digital_Banking_Sector - An overview of cyber security in digital banking sector