International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 12 Issue 5, May, 2023, Impact Factor: 7.751

Cyber Security of Banks in India

Medicherla Sri Sivathmika[1], J.V. Satyanarayana[2*], Josyula Sai Manogna[3]

[1] Symbiosis Centre for Management Studies, Pune, Maharastra, India
[2,3] R.V.R & J.C. College of Engineering, Guntur-522019, Andhra Pradesh, India

*Corresponding author: drjosyula27@gmail.com ttps://orcid.org/0000-0002-6834-2336

ABSTRACT

This research paper and study is all about cyber security of banks in India. The daily volume of transactions handled by internet banking is in the trillions. Due to a rise in cyber security breaches brought on by the exponential growth in transactions, clients are suffering financial losses. There must be a user-leaved susceptibility that is exploited by external threats from attackers for any risk to develop. In any attack, the living human is the initial centre of focus, and how he reacts to that always determines the severity of the subsequent losses. In today's digital environment, e-banking channels may be a blessing if they are used properly, with appropriate caution, and in accordance with all cyber security best practices. This article uses primary data to analyze the association between demographic factors and cyber security measures taken by E-banking customers with accounts at various Indian banks. The survey shows that people are very vulnerable to cyber security risks and vulnerabilities regardless of their age, education level, or gender. Bank's attempts to inform consumers via education emails and messages fall short of raising their level of knowledge of numerous hazards and security lapses. Banks are recommended to promote tailored secure E-banking methods in addition to bulk mailings.

Keywords: Cyber Security, E-banking, Cyber threats.

INTRODUCTION

In recent years, the demand for cyber security products and services has increased across industries. Cyber security refers to the organization of technologies, procedures, and methods designed to prevent networks, devices, programs, and data from attack, damage, malware, viruses, hacking, data thefts or un authorized access. The increasing reliance on the Internet for carrying out complex banking and financial transactions has caused a lot of concern in regards to the integrity of these networks, which are continuously targeted by hackers. It is important that proper strategies and solutions are in place to safeguard banking platforms from potential threats and vulnerabilities. Cyber security solutions need to be brought into play, which can ensure the safety of the user's personal and financial details.

Cyber security is a major concern for every business organization. There are recent findings that states that cyber security breaches have increased by 50% in the past year alone. Cyber security is not only restricted to IT organizations, it is important for every single business. But, for banks, it holds important value. Banks deal in millions of transactions on a regular basis. Hence, it is very important for banks to take protective security procedures to safeguard their data against cyber attacks. As per a COWEN AND COMPANY report, banks breach occurs in over 120 million cases per year. The growing number of cyber attacks on financial institutions have led to a significant increase in the demand for cyber security solutions that can help mitigate the risks associated with these attacks. Financial institutions have developed sophisticated technology and monitoring techniques to help ensure their customers' safety while offering the convenience of online banking. They use multifactor authentication, encryption, privacy policies and training, anomaly detection, and other methods of securing customer data. Customers also play an important role in protecting financial information through education and the use and regular updating of technological protections such as anti-virus software, anti-spyware, and firewalls.

LITERATURE REVIEW

Emergence of Fintech and cyber security in a global financial centre: Strategic approach by a regulator.

Research Framework: This study intends to investigate the strategic articulation of such opportunities and dangers by the regulator of a global financial centre (GFC) in the context of a global trend toward the use of Fintech.

Research Gap: Fintech is not conclusive in this examination of the performance and efficacy of the financial regulator's strategic strategy because it has only recently and swiftly evolved. A longitudinal approach may be used in future research to study and examine the regulatory actions made by financial regulators during various GFCs.

A study of cyber-defense strategies adopted by major Public and Private sector Banks of India:
Research Framework: The research compares private and public sector banks to see what they're doing to safeguard themselves from cyber-attacks. The Reserve Bank of India's reports and the annual reports of India's top public and private sector banks were used to compile secondary data. The findings have consequences for banks in terms of evaluating their cyber-security regimes.

Research Gap: Since networks are used to conduct crucial activities, computer security is a large topic that is getting more significant as the globe becomes more interconnected. With each New Year that goes by, cybercrime continues to take different turns, and the security of the information also does. This study has some restrictions like no clear-cut solutions for the problem, lack of survey conduction and more.

The Significance of Cyber security System in helping managing Risk in Banking and Financial Sector:
Research Framework: This study's goal is to illustrate the importance of cyber security and its advantages in organizational systems, with a particular emphasis on the banking industry. Additionally, this study intends to promote the use of cyber security to retain information securely and manage information risk. However, many banking and financial institutions continue to be cautious when it comes to applying and utilizing cyber security. In fact, it's possible that these financial organizations are ignorant of the advantages of cyber security.

Research Gap: This study has several restrictions. The amount of feedback that was gathered from the questionnaire is an important factor, as more responses would have enhanced the value of this study. Despite the aforementioned limitations, the study's findings are important for Bahraini banking and financial institutions because they can be used as guides to enhance their staff member abilities in spotting various cyber-attacks. These results are also very significant for expanding our understanding of cyber security and how it affects these financial institutions.

RESEARCH METHODOLOGY

Quantitative and qualitative Research method is used in the research Paper. The data on cyber security provided by banks to protect their customers and data gives us an insight on how banks protect their customers information, kinds of cyber security they use, how they work and whether customers are aware or not.

Cyber security in banking sector, data handling is ensured with security and transparency. Financial institutions utilize sophisticated monitoring tools, firewalls, and other security measures to protect consumer information. These measures include multifactor authentication, encryption, privacy policies and training, anomaly detection, and more. Through education, the use of technological measures like firewalls, anti-virus software, and anti-spyware, as well as their routine upgrading, customers can play a significant part in ensuring the security of financial information.

Type of Research Design: Descriptive and Exploratory research design is the type of research design used in the research paper. Cyber security in banking and finance needs description about the various aspects of the topic. Introduction of cyber security provided by banks, its uses in banking and finance sectors and how aware the customers are of it.

Cyber security is the use of individuals, procedures, technology, and policies to protect businesses, their critical systems, and sensitive data from internet attacks. Incidents involving cyber-risk can have costly operational, financial, reputational, and strategic effects on a company. Because of this, the effectiveness of current security measures has decreased, and most firms now need to step up their cyber security efforts.

Sources of Data
1. Survey: We conducted one online survey through which we had about 100+ responses. We had different age groups in the survey to see if age plays any part in if the customers know about their banks cyber security measures. We also had different banks in the survey to find that whether the banks also play role in making their customers aware about their cyber security measures.

2. Research Papers: Research Papers on cyber security provided by banks, requirements of cyber security, cybercrime etc. These articles' major readers were other professionals. In these papers, original research or case studies were often provided. Many of these articles have undergone "peer review" or "refereeing." This indicates that research and findings are evaluated by academics in the same subject before an article is published. The majority of the time, articles in scholarly publications were I written by and for faculty, researchers, or other subject-matter experts (ii), (iii) used scholarly or technical language, (iii) included a complete bibliography of all the sources cited in the conducted two online interviews with managers of HDFC and Union Bank respectively. The interviews were conducted through the Google meet platform. We prepared a questionnaire to ask them specific article, and (iv) frequently underwent peer review (refereed). These papers ranged from the need for cyber security and how cyber security is helping banks.

3. Journal Articles: Various journal articles were studies for the purpose of the research paper. These were business journals and conference papers. Proceedings of a conference included compilations of conference papers, research, and information. Proceedings were frequently the initial publication of research that later appeared in a scholarly publication, and they occasionally underwent peer review.

4. Interviews: We questions regarding cyber security their banks provide and how their customer can know more about it.

Variables

Dependent Variable: The driving force behind a researcher's decision to undertake study or produce a final interpretation. The need for cyber security in Banking and Finance would be the dependent variable in this study.

Independent Variable: The variable that impacts the dependent variable to arrive to the final result. Understanding what cyber security is mostly used and the ways it's being applied would be the independent variable in this study.

Discrete Variable: The one that has a clear quantitative interpretation but can only accept specific numeric values (rather than any number in an interval). Age is a factor in whether a person understands about the risks regarding cyber security.

Nominal Variable: A nominal variable is a variable that is used to name, label, or categorise specific measurements. Women are more likely than men to receive fraudulent calls and fall victim to them. To find out who is more susceptible to phishing and scam calls, we used gender as a variable.

Tool: The p value and f value were determined using the IBM SPSS data analytical tool to determine whether the presumptive hypothesis was true.

Data: The data collected for the purpose of this research paper was through surveys, research papers, journal articles and interviews on Cyber security provided by banks to their customers and its uses in Banking and Finance sector. The data was qualitative and quantitative in nature which gave insights about the topic.

Number of Observations: To collect the appropriate data, approximately 23-25 research papers were studied, out of which, the most informative and accurate 18 papers to my research paper, were selected. The papers which gave more focus on application of Cyber security by Banks and the current need for cyber security in online banking were preferred.

Time Period: We collected and analyzed recent data from the past 2-3 years. This was taken as secondary Data.

Objectives

1. To research how well-informed e-banking facility customers are about threats and vulnerabilities.
2. To examine how responsive cyber security hazards are among those who utilize online banking services.

Hypothesis

1. The responder population in terms of vulnerability to cyber security threats varies significantly by age group.
2. There is a large difference between vulnerability and education of the people
3. The vulnerability of each gender to cyber security risk varies significantly.

Data Analysis and Interpretation

It is important for banks to protect its customers from different types of cyber threats, since they not only affect the banks data but also the following:

CLIENT LOSS: Cyber attacks are no longer a matter of data security. They are now affecting the bank's status and causing loss to its customers' assets. Normally, when a user loses money due to card fraud, it can be retrieved from the bank. But, in circumstances like data infringement, it takes time to retrieve the funds. This is very worrying for customers. To keep customer's data safe, every bank needs to execute cyber security methods that can safeguard their customers' data.

BANK'S STATUS: Data breaches are becoming a regular occurrence for banks. This is due to the increased number of attacks on banks and their customers. A data breach can be defined as an incident in which an attacker gains access to confidential information or otherwise compromises a system. The main reason for this is that most of the current security measures are weak, especially when it comes to online banking. Banks should evaluate their current security measures and implement new ones if necessary to protect their customers from cyber attacks.

DIGITIZATION: Almost everything has now been digitized, as we all know. We rely on multiple digital channels for everything from ordering things to scheduling meetings and sending money. This makes it critical for banks to improve their customer-facing banking activities, since hackers may quickly get access to banking applications if suitable cyber security measures are not implemented.

TOP CYBER THREATS FACED BY BANKS

- Bank's Reputation
- Digitization
- Phishing
- Malware
- Unencrypted Data
- Spoofing
- Data Manipulation

PRIMARY DATA ANALYSIS

We saw that the frauds happen in broad daylight. Nowadays, between the hours of 7 a.m. and 7 p.m., 65 to 70 percent of cybercrimes occur. Contrary to what many people think, scams do not frequently happen during strange hours of the night. In addition, we found that 80-85 percent of the affected consumers are between the ages of 22 and 50, which is regarded as a tech-savvy age group.

Table-1.A.

Gender	Frequency
Male	50
Female	Female

TABLE-1.B.

Age Group	Frequency
18-25	29
25-35	13
35-45	24
45-55	24
55 and above	10

TABLE-1.C.

Educational background	Frequency
12th pass	2
Under Graduate	47
Post Graduate	40
Doctorate	4
Others	7

TABLE-1.D.

E-banking mode used	Percentage
Internet banking	71%
POS	16%
Mobile e-banking	52%
Pay tm wallet	37%
UPI	73%

TABLE-1.E

Banks used for transactions	
HDFC	22
Union Bank	5
State Bank of India	21
ICICI Bank	26
Canara Bank	5
others	21

TABLE-1.F

Period of using e bank mode	
Less than a month	8
1month-6 months	6
6 months- 1 year	9
More than 1 year	77

Table-1 Source- Primary data

We found that fraudsters are frequently compensated employees who are regarded as knowledgeable. In addition, we found that males are more frequently the victims of frauds than women. This makes it impossible to apply the problem generally.

According to the profile study, consumers who use e-banking platforms for operations are most likely to be between the ages of 18 and 25. This group accounted for 29% of the sample size, followed by customers between the ages of 25 and 35 and those between 35 and 45. The majority of clients, or 47%, are undergraduates, followed by 40% of customers who are postgraduates, and 2% of respondents were 12th graders. These individuals were all comfortable using online banking methods. Each client was utilising at least one of the methods to conduct internet banking.UPI is the preferred method of transaction for the greatest percentage of respondents (73%) followed by Internet Banking (used by 70%). Since 77 percent of consumers have been using one of these channels for more than a year, the sample demonstrates that e-banking is no longer a novel approach for customers. Rather, it has grown in popularity. At the time of data collection, just 8% of customers had never used an e-banking option before and had only recently enrolled.

H1: The responder population in terms of vulnerability to cyber security threats varies significantly by age group.

Table-2, Source- SPSS Software

S. No	Vulnerability type	F value	P value
1.	Utilising free public Wifi and using public computers to browse the internet	2.793	.029
2.	Use the free public Wi-Fi to conduct online banking activities.	4.643	.002
3.	To customize the mobile device's operating system utilities, hack or unlock it.	3.133	.017
4.	Install apps that give the most bonuses and savings.	3.760	.006
5.	Access any links you've received via email or sms.	3.277	.013

We agree the H1 because the p value is less than 0.05 and the sample in Table 2 has provided supporting evidence for it. We have a 95% confidence level that the vulnerability of respondents in different age groups to the various cyber security dangers mentioned above varies. Users between the ages of 18 and 35 are more vulnerable to the risks associated with using free public wife and using public computers to access the internet. Free public Wi-Fi is made available in airports' hotels, coffee shops, and train stations, among other places, however it exposes users to a number of covert risks. Free Wi-Fi access points may also be "rogue access points," which deceive users into connecting to what they believe to be a trustworthy network since the name seems well-known and reliable. Young people in the age range of 18 to 25 are also more susceptible to downloading unidentified applications where the greatest incentives and discounts are provided and the threat of jail breaking or rooting the mobile device to change the computer system. Without understanding the security dangers, they want to have more access to the device so they can enjoy the more functions. When an IOS device is hacked or an Android smart phone has remote access, the authorized administrator can use many of the device's intriguing features. Additionally, it renders them more vulnerable to nefarious assaults. The manufacturer locks the operating systems of mobile devices so that users only have access to limited privileges. The user is intended to be protected from harmful assaults with the help of this. Any assault that is skilled enough will be able to enter a user account with administrator access, giving it complete control to do whatever with data. Younger users reply to phishing emails by clicking on unexpected links they receive. These are perception management techniques where fraudsters pretend to be reliable sources to entice victims into clicking a link or downloading a malicious programme. Users run a higher risk of downloading malicious software when they click on unconfirmed links or download dubious programmes. Users over the age of 35 are less likely to download new applications or click on links or emails, which helps them protect themselves against assaults. Age plays a big part in how people react to these risks, according to statistics.

H2: There is a large difference between vulnerability and education of the people

S. No	Vulnerability type	F value	P value
1.	Utilize your phone's auto-lock or timer feature.	1.148	.337
2.	After using a public Wi-Fi network to access the internet, change your online bank passwords.	1.649	.166
3.	Update software patches often and install the most recent versions of the operating system.	1.020	.399
4.	Installing antivirus protection on your phone.	1.145	.338
5.	storing private information on a mobile device, such as a debit card, Andhra, or Pan Card	.766	.549
6.	Sensitive data stored on mobile device is password-protected.	1.434	.226

Table-3, Source- SPSS Software

We refute H2 because the sample in Table 3 provides sufficient evidence and all of the parameters have p values larger than 0.05. Customers of all educational levels do not auto-lock their mobile devices for convenience of use and operational simplicity. Even after utilizing public Wi-Fi to conduct financial transactions, many do not reset their passwords. Customers underestimate the security risk associated with credentials that are collected over public Wi-Fi, which increases the likelihood of cyber crime. Cyber - criminals may purchase specialized software packages and even hardware to aid them in listening in on Wi-Fi transmissions. This tactic can provide the attackers access to everything users do online, including any data they may have entered into forms when browsing websites, login details, and even the ability to take over users' accounts. Therefore, using free Wi-Fi to input credentials to conduct online banking transactions is exceedingly risky. After completing the transaction over public Wi-Fi, it is very important to take special care to update the login information right away. Web users banking are hesitant to upgrade the operating system on their mobile device to the most recent versions, and they often install operating system patches.

By failing to install appropriate antivirus software on their mobile device, all users leave their systems equally exposed. When all users regularly save their sensitive data (debit card, Aadhar, and Pan Card) on a mobile device for later use without password protection in an unencrypted form, education is irrelevant. Thus, we draw the conclusion that education degree does not significantly affect the vulnerability to cyber attack threats.

While employing E-banking methods, we investigated the connection between gender and response to security awareness. We have 95 percent confidence that both genders are similarly exposed to cyber security hazards based on the data provided by the sample in Table 4. Based on gender, there is no difference in the awareness of adhering to the guidelines for secure E-banking transactions. We accept H3 since it has a p value larger than 0.05 in all circumstances.

H3: The vulnerability of each gender to cyber security risk varies significantly.

Table-4,Source- SPSS Software

S. No	General security awareness tips	F value	P value
1.	Giving bank login information over the phone.	.580	.677
2.	Before inputting any personal or financial information on any website, be sure that it is secure and genuine.	1.419	.240
3.	Through emails, information regarding phishing, viruses, etc. spread.	.391	.759
4.	Comparison of bank statements and SMS notifications received from the bank	1.830	.127
5.	Passwords for online banking are kept short and easy to remember.	2.336	.059
6.	revealing passwords to bank employees in order to do internet transactions.	2.441	.050
7.	sharing online transaction passwords with friends, family, and coworkers	2.211	.071
8.	In case the passwords were shared, immediately change them.	0.193	.942

Customers of any gender may fall prey to scam calls. People readily comply with requests for sensitive information when cybercriminals pose as authorized bank employees. Customers do not verify a website's security and validity before entering any personal or financial information. They use easy-to-remember, basic passwords that are easily cracked by brute-force assaults. Social engineering assaults affect people. Fewer people are aware of phishing, malware, or any other kind of cyber security assault that might cause them to lose money through their mobile devices. The most popular tool used to carry out online scams is phishing mail, in which the sender poses as a well-known individual, bank, or government agency in order to get sensitive information. The outcome demonstrates that gender has no bearing on answering phishing emails, which subsequently carry out different dangerous tasks including launching malware or Trojans to steal data. Customers, regardless of gender, tend to be less knowledgeable about fundamental security precautions including changing passwords after sharing them, comparing bank statements and online transactions, and reviewing transaction notifications sent to mobile devices. Banks are required to notify consumers by SMS on their registered cell phone number and email address. For users, these warnings serve as the finest navigation for spotting fraudulent behavior. If a suspected alert about behavior that the user did not perform is notified as soon as possible to the bank's call center or help desk number, the bank may be able to address the issue more quickly and add any missing cash to the user's account. To stop subsequent attacks, it can also instantly ban the account. Our survey reveals that both genders equally lack general safety awareness.

Interviews of HDFC bank and UNION bank managers:

HDFC Branch- Vivekananda Nagar branch: In this interview, we asked Mr. Nagendra to give us a few insights on the current cyber security measures HDFC takes and those the branch follows. The following was said by him:

1. Pin security- it is obtained in random by the system
2. Additional authentication
3. Virtual keyboard
4. Insta-alerts

HDFC also created awareness programs in different parts of the state including Vivekananda Nagar colony, about the cyber security threats. More than 500 people were present in this campaign."

UNION BANK- Nizampet Branch: Mr. Shiva churapalli was interviewed about the same about the cyber security measures and if any programs were conducted.

CYBER SECURITY OF INDIA

The previous few years have witnessed a number of important and unusual incidents in India, which have elevated the concern over cyber security for the country's banking industry to a new level. The Government of India's continuing Endeavour, through its flagship Digital India programme, has been the most major driver in this respect. Reserve Bank Information Technology Pvt Ltd (ReBIT) has been set up by the Reserve Bank of India (RBI), to take care of the IT requirements, including the cyber security needs of the Reserve Bank and its regulated entities. ReBIT will focus on IT and cyber security (including related research) of the financial sector and assist in IT systems audit and assessment of the RBI regulated entities; advise, implement and manage internal or system-wide IT projects (both the existing & the new) of the Reserve Bank as mutually decided between the Reserve Bank and ReBIT. ReBIT has the potential to guide the regulated businesses in the IT aspects of their operations as well as for the RBI's IT related functions and projects, acting as a catalyst for innovation, huge systems, and new ideas. ReBIT will actively contribute to the establishment of standards to increase the Reserve Bank's position as a regulator given the requirement for connectivity and inter collaboration.

CONCLUSION

The majority of this study's findings suggest that regular users of e-banking channels are uninformed of the dangers and inherent cyber security hazards they face when doing online banking activities. Even after having a much better level of knowledge, the majority of users are unaware of the hidden danger hidden behind freebies, discounts, and websites that closely resemble the genuine sites of banks, governments, and other institutions. There is a good chance that the careless clients won't notice money being taken from their account. Customers frequently lose the struggle since it is impossible to reverse funds once they have been spent because they failed to instantly compare bank SMS notifications with their digital passbook balance to verify for permitted transactions. When well-educated people are easily tricked by cybercriminals, it calls into question the security of internet banking and weakens the system's defences. Attacks and the potential for fraud (phishing) data breach make it difficult for internet banking to expand. If cyber scams are not stopped, Urban Cooperative banks risk losing customers. Users must be regularly reminded to observe safety precautions when using electronic banking channels through continuous customer awareness and feedback.

Recommendations: Individual understanding of cyber security dangers including social manipulation, phishing, vishing, Trojans, and malware assaults may be increased with short quizzes with incentives. One step towards lowering the likelihood of fraud happening is to give clients accurate and sufficient information about security best practices when they visit bank websites or connect into digital applications. To raise student knowledge of security, it is necessary to make cyber security themes required in academic courses at all levels of education. The banks should make frequent use of social media to promote security measures that may be integrated as a lifestyle measure when utilising e-banking channels.

REFERENCES

[1]. Dam, L. (2020). Relationship between Demographic Variables and Awareness on Cyber security hreats: An Empirical Analysis. The Orissa Journal of Commerce, 41, 112-122.
[2]. Sarihaddu, M. N. K., & Linde, I. (2022). Evaluation of the performance of the HR management and Cyber Security in Banking sector communication and development of interdisciplinary competences in the digital age, 107.
[3]. Shah, P., & Agarwal, A. (2020). Cyber security behaviour of smart phone users in India: an empirical analysis. Information& Computer Security, 28(2), 293-318.
[4]. Parmar, S. D. (2018). Cyber security in India: An evolving concern for National security. The Journal of Intelligence and Cyber Security, 1(1).
[5]. Jibril, A. B., Kwarteng, M. A., Chovancova, M., & Denanyoh, R. (2020, March). Customers' perception of cyber security threats toward e-banking adoption and retention: A conceptual study. In ICCWS 2020 15th
[6]. International Conference on Cyber Warfare and Security (Vol.270). Academic Conferences and Publishing limited.
[7]. https://www.vu.edu.au/about-vu/news-events/study-space/5-easy-ways-to-protect-yourself-from-cyber-attacks
[8]. https://rebit.org.in/whitepaper/emerging-trends-and-challenges-cyber-security
[9]. https://www.ibm.com/in-en/industries/banking-financial-markets/cyber- security
[10]. https://www2.deloitte.com/in/en/pages/financial-services/articles/in-fs-cybersecurity-in-the-indian-banking-industry.html
[11]. https://intellipaat.com/blog/cyber-security-in-banking/