Cyber Security Initiatives in Banking Sector: A Correlational Analysis

Dr. Monty Kanodia[1], Dr. Shilpi Saxena[2] & Ms Priya Gupta[3]

Abstract

Cybercrime in the banking sector encompasses a wide range of malicious activities aimed at exploiting vulnerabilities in financial institutions' digital infrastructures. These crimes include hacking, phishing, malware attacks, identity theft, and financial fraud. Cyber criminals target banks to steal sensitive customer information, disrupt operations, and siphon funds. The impact of such attacks can be severe, leading to financial losses, reputational damage, and erosion of customer trust. Banks must continually adapt their cyber security strategies to defend against evolving threats, implementing advanced technologies and robust protocols to protect their systems and data. This study empirically examines association between customer awareness of cyber security initiatives and satisfaction regarding cyber security initiatives in banking sector. For empirical analysis of association between the variables of the study, correlation technique was applied on primary data collected through a sample of 101 respondents. The study concluded in a positive association between cyber security initiatives taken by banks and customers satisfaction arising out of those initiatives.

Keywords: Cyber Security, Hacking, Phishing, Malware Attacks, Customer Satisfaction.

Introduction

Cyber-crime in online banking involves the use of technology to commit illegal activities targeting financial institutions and their customers. As online banking has surged due to its convenience and efficiency, it has also become a prime target for cybercriminals. These criminals employ various tactics, such as phishing, malware, ransom ware, and data breaches, to gain unauthorized access to sensitive financial information and commit fraud.

1 Asst. Professor- SG, Dept. of Commerce, IIS (Deemed to be University), Jaipur
2 Assistant Professor-SG, Dept. of Commerce, IIS (Deemed to be University), Jaipur
3 Student, IIS (Deemed to be University), Jaipur

Cyber-attacks are malicious attempts by individuals or groups to compromise, damage, or gain unauthorized access to computer systems, networks, or devices. These attacks can lead to significant financial, operational, and reputational damage for individuals, organizations, and governments. Cyber-attacks pose a significant threat in today's digital world, targeting individuals, businesses, and governments. Awareness of common attack methods, understanding their potential impacts, and implementing basic security measures can help mitigate these risks and protect valuable information and assets.

Phishing schemes often involve sending deceptive emails or creating fake websites that appear legitimate to trick individuals into revealing personal information, such as login credentials and account details. Malware can infect computers and mobile devices, capturing keystrokes or stealing data directly. Ransom ware attacks encrypt critical data and demand payment for its release, causing significant disruptions to banking operations.

The consequences of cyber-crime in online banking are severe, ranging from financial losses and identity theft to reputational damage for financial institutions. Banks must constantly upgrade their cyber security measures, including employing encryption, multi-factor authentication, and real-time monitoring, to safeguard against these evolving threats. Additionally, educating customers about safe online practices is crucial in the fight against cyber-crime. As technology continues to advance, so too the strategies and collaborations among banks, cyber security professionals, and regulatory bodies to protect the integrity of the online banking system.

Cyber security awareness refers to the knowledge and practices that individual and organizations must adopt to protect themselves from cyber threats. It involves understanding the various types of cyber risks, recognizing potential threats, and implementing best practices to safeguard information and systems. cyber security awareness is a critical component in the defence against cyber threats. By educating individuals about potential risks and promoting best practices, both organizations and individuals can significantly reduce their vulnerability to cyber-attacks. Continuous education, proactive strategies, and a culture of security are essential to maintaining a robust cyber security posture.

Literature Review

Cele & Kwenda (2024) discussed in their paper that in recent years, the

rapid evolution of digital technologies has transformed the banking sector, providing customers with unprecedented convenience and accessibility through digital banking (DB) services. South Africa, and other developing nations, has embraced these advancements to meet the demands of its increasingly tech-savvy populace. Yet, the rise in cybersecurity threats presents a pivotal challenge, influencing the broader acceptance of these services. Rao, P.B. (2024) explored evolving cybersecurity challenges in online banking, focusing on risks, regulations, and emerging technologies for enhanced security in their work. Nalini, R., & Yuvasri, S. (2024) explored the impact of digital transformation on customer experience in banking, focusing on technologies like mobile apps, AI, and blockchain. A survey of 350 digital banking users in Tirunelveli was conducted to assessed service quality across banking sector. Data analysis using Chi-square and SPSS revealed variations in service quality across banks. Johri & Kumar (2023) in his work highlights the critical role of customer awareness in combating cybersecurity challenges within the banking sector. The research emphasizes the importance of regular customer training initiatives aimed at bolstering security measures and alleviating customer apprehensions regarding security. It finds that increased cyber security awareness significantly boosts customer satisfaction with digital banking service. Kumar, M. (2023) in his study reviewed global trends in cyber threats targeting digital banking. It analyzed unencrypted data, phishing, and malware issues, proposing integrated security and customer awareness as solutions. Results emphasize widespread risks, especially from insufficient security practices and low public awareness, urging better encryption and user education for secure banking. Alzoubi et al. (2022) recommended based on their research findings that financial institutions enhance their cyber security protocols to protect against vulnerabilities exploited by hackers. Malik & Islam (2019) conducted a study in Pakistani banking sector which reveals a notable adverse effect of cybercrime on organizational effectivenessTop of FormBottom of Form and customer satisfaction. The authors recommend that banks implement robust cyber security measures and regular training programs to improve customer trust and satisfaction. Normalini & Ramayah (2019) in a study examines how factors related to security perception, including authentication, confidentiality, and data integrity, influence customers' readiness toTop of FormBottom of Form use Internet banking services. The findings showed that these security perceptions are crucial for maintaining customer trust and satisfaction in digital banking. Das, S., & Nayak, T. (2013) in their work elaborated the concept of cybercrime and highlighted its impact on society. Thus, based on literature review it could be concluded that cyber security is an alarming issue in banking sector which requires serious attention for customer satisfac-

tion and retention.

Objectives of the Study

This study has been conducted keeping in view the following objectives:

1) To gain an insight into the field of cyber-crime in banking sector.

2) To analyse the banking customer's awareness level regarding cyber security initiatives taken by banks.

3) To determine association between awareness level regarding bank's cyber security initiatives and banking customer's satisfaction level.

Hypothesis of the study

H_0: There is no association between Cyber Security initiatives taken by banks & satisfaction level of customers of banks.

H_a: There is significant association between Cyber Security initiatives taken by banks & satisfaction level of customers of banks.

Research Methodology

The research study is empirical, descriptive and quantitative in nature. The study was conducted with a sample of 101 respondents who are using banking services from at least last 2 years. Demographic details of respondents are shown in table 1 below. The study participants were selected using a judgmental sampling approach. The study findings rely on primary data gathered through a structured questionnaire distributed among respondents from Jaipur city.

The structured questionnaire, developed with insights from existing literature, was employed to gather data from respondents. The questionnaire comprised of questions focusing on awareness of cyber-attacks, hacking, and phishing activities, which commonly affect users and turn them into victims of such threats. The questionnaire also included questions regarding customers' satisfaction with the cyber security assistance provided by banks. Responses were measured using a five-point Likert scale, where

1 indicated strong agreement and 5 indicated strong disagreement. Pearson's correlation was used to analyse the data and analysis was done using SPSS software.

Findings of the Study

Awareness Level regarding cyber security Initiatives in banking sector

One of the objective of the study is to analyse the banking customer's awareness level regarding cyber security initiatives taken by banks. The findings of the study drawn on the basis of descriptive statistics shown below in table 1.

Table 1: Awareness regarding cyber security initiatives

Descriptive Statistics			
	N	**Mean**	**Std. Deviation**
Are you familiar with the concept of cyber-crime in online banking?	101	2.0198	1.30369
Are you aware that victim of fraud and cybercrime should report it to Action Fraud?	101	2.3465	1.47266
Are you aware about the phishing e-mail, pop up, etc. should not be opened as they may steal your banking data?	101	1.9010	1.26890
Rate your awareness about the hacking in online banking?	101	2.1089	1.19081
Are you aware that password can be strengthened by combination of alphanumeric characters, Special characters, length of the password?	101	1.7327	1.20740
Are you aware that by installing anti-virus in your system, you can save your banking information?	101	2.0594	1.34775

Are you aware about the Information Technology (Amendment) Act, (IT Amendment Act)	101	2.8614	1.52990
Are you aware that firewall software in your system protect you from cyber crime	101	2.1980	1.31924
Valid N (listwise)	101		

Source: Primary Data

The Table 1 summarizes descriptive statistics on awareness levels regarding cyber security initiatives in the banking sector among 101 respondents. Overall, awareness levels range from moderate to low, with some variation among different aspects. Familiarity with cyber-crime in online banking scored a mean of 2.0198, reflecting moderate awareness, though there is notable variation (SD = 1.30369). Awareness of procedures for reporting cybercrime was slightly higher (mean = 2.3465, SD = 1.47266). Awareness of phishing risks and hacking in online banking was moderate, with mean scores of 1.9010 and 2.1089, respectively, both showing variability in participant understanding. Awareness about strengthening passwords was the lowest (mean = 1.7327, SD = 1.20740), indicating limited knowledge on password security practices. Awareness of anti-virus software's role was moderate (mean = 2.0594, SD = 1.34775), while awareness of the IT (Amendment) Act was the highest (mean = 2.8614, SD = 1.52990), though respondents showed varied understanding of it. Awareness of firewall software scored moderately as well (mean = 2.1980, SD = 1.31924). These findings reveal moderate to low awareness across various cyber security aspects, with notable variation among respondents. Awareness of the IT (Amendment) Act is highest, while password security practices are less well-known.

Satisfaction level from cyber security initiatives in banking sector

The another focus areas of study is to find out satisfaction level of customers towards cyber security initiatives in banking sector. Table 2 below shows descriptive statistics of satisfaction level of customers.

Table 2: Satisfaction level from cyber security initiatives in banking sector

Descriptive Statistics			
	N	Mean	Std. Deviation
Are you satisfied with the services provided by the bank on cyber-crime?	101	2.4752	1.14537
Are you satisfied by protection of firewall software?	101	2.3267	1.14113
Are you satisfied by the laws provided by government for prevention of cyber-crime?	101	2.6634	1.15998
Are you satisfied with the services of online banking working 24/7 for prevention of cyber-crime?	101	2.2673	1.19072
Are you satisfied with the camping's by government regarding awareness of cyber crime	101	2.5248	1.25375
Valid N (listwise)	101		

Source: Primary Data

The table 2 above, provides an analysis of satisfaction levels regarding cyber security initiatives in the banking sector, based on responses from 101 participants. Overall, satisfaction is moderate, with mean scores ranging from 2.2673 to 2.6634, reflecting varied levels of contentment. Respondents reported the highest satisfaction (mean = 2.6634, SD = 1.15998) with government-led cybercrime prevention laws, though there is notable variability. Satisfaction with government campaigns to raise cybercrime awareness was also relatively high (mean = 2.5248, SD = 1.25375). In contrast, satisfaction with 24/7 online banking services for cybercrime prevention and firewall protection was somewhat lower (means of 2.2673 and 2.3267, respectively), suggesting opportunities for enhancement in these areas.

Association -Awareness level regarding bank's cyber security initiatives and Customer Satisfaction

The association between awareness level regarding bank's cyber security

initiatives and satisfaction level of customers was tested by formulating the hypothesis which is shown below. Pearson correlation was used to find out the association between two variables. The result of correlation is shown in table 3.

H_0: There is no association between Cyber Security initiatives taken by banks & satisfaction level of customers of banks.

H_a: There is significant association between Cyber Security initiatives taken by banks & satisfaction level of customers of banks.

Table 3: Correlation

		Awareness regarding cyber security Initiatives	**Customers Satisfaction**
Awareness regarding cyber security Initiatives	Pearson Correlation	1	.692**
	Sig. (2-tailed)		.000
	N	101	101
Customers Satisfaction	Pearson Correlation	.692**	1
	Sig. (2-tailed)	.000	
	N	101	101

**. Correlation is significant at the 0.01 level (2-tailed).

Source: Primary Data

Correlation is a statistical measure used to describe the relationship between two variables, indicating both the strength and direction of their association. The correlation coefficient (r) ranges from -1 to 1, with values closer to ±1 representing stronger relationships. In this study, the correlation coefficient (r) is calculated to be 0.692, indicating a moderately strong positive relationship between the two variables under investigation. This means that as awareness of cyber security initiatives increases, customer satisfaction also tends to rise. The study's significance level is set at 1% (0.01), and with a p-value of 0.000, the results are statistically significant,

leading to the rejection of the null hypothesis. Therefore, there is a meaningful positive correlation between cyber security initiatives by banks and customer satisfaction. These findings suggest that enhancing cyber security measures and awareness programs could effectively boost customer satisfaction, underscoring the importance for banks to continually educate customers on cyber threats and prevention measures to strengthen trust and satisfaction.

Conclusion

In conclusion, this study highlights the moderate to low levels of customer awareness regarding various cyber security initiatives in the banking sector, with the highest awareness found in the area of the IT (Amendment) Act and the lowest in password security practices. Satisfaction with these initiatives was similarly moderate, with customers expressing the greatest satisfaction with government-led cybercrime prevention laws, while 24/7 online banking security services and firewall protection received lower satisfaction scores, pointing to potential areas for improvement. The positive correlation ($r = 0.692$) between awareness and satisfaction levels suggests that as customers become more informed about cyber security measures, their satisfaction with these initiatives increases. This significant relationship underlines the need for banks to invest in continuous awareness programs and educational campaigns around cyber security. By enhancing customer knowledge on cybercrime prevention, banks can not only increase satisfaction but also foster greater trust and loyalty, ultimately strengthening the relationship between banks and their customers.

In future, studies exploring the evolving role of AI and machine learning in enhancing cybersecurity within the banking sector can be conducted. Additionally, cross-industry comparisons and the study of emerging cyber threats offer significant potential for advanced studies in this field.

Limitations of the Study

The findings of study are based on respondents from Jaipur city only. Conducting the study solely in Jaipur limits its geographical scope, making the findings less applicable to other regions. Also short time span of the research may hinder the capture of long-term trends or evolving cyber threats. The study is a generalized study of cyber security initiatives ad-

opted in banking sector. Lacks of focus on specific banks' initiatives weakens the ability to analyze detailed, bank-specific strategies, resulting in more generalized conclusions about cybersecurity efforts.

Recommendations

Based on the study's findings of positive association between cybersecurity initiatives and customer satisfaction, banks should prioritize strengthening their cybersecurity infrastructure. Implementing advanced security protocols, such as multi-factor authentication and encryption, can enhance customers' trust. Regularly updating security systems to address emerging threats will maintain customer confidence. Banks should also focus on transparent communication, informing customers about the measures taken to protect their data. Offering educational programs on cybersecurity can empower customers to safeguard their personal information. Additionally, rapid response teams for cyber incidents and ensuring compliance with regulatory standards can further improve customer satisfaction and loyalty.

References

Alzoubi, Y. I., Al-Ahmad, A., Kahtan, H., & Jaradat, A. (2022). Internet of things and blockchain integration: security, privacy, technical, and design challenges. *Future Internet, 14(7), 216.*

Cele, N. N., & Kwenda, S. (2024). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime*.

Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. *International journal of engineering sciences & Emerging technologies*, *6*(2), 142-153.

Johri, A., & Kumar, S. (2023). Exploring customer awareness towards their cyber security in the Kingdom of Saudi Arabia: A study in the era of banking digital transformation. *Human Behavior and Emerging Technologies*. 2023(1), 2103442.

Kumar, M. (2023). An overview of cyber security in digital banking Sec-

tor. *East Asian Journal of Multidisciplinary Research.* 2(1), 43-52.

Malik, S. U. F., Mahmud, Z., Alam, J., Islam, M. S., & Azad, A. K. (2019). Relationship among obesity, blood lipids and insulin resistance in Bangladeshi adults. *Diabetes & Metabolic Syndrome: Clinical Research & Reviews. 13(1), 444-449.*

Nalini, R., & Yuvasri, S. (2024). A Study on the Impact of Digital Transformation in the Banking Sector on Customer's Experience. *International Journal of Innovative Research in Engineering and Management*. 11(2), 40-44.

Normalini, M. K., Ramayah, T., & Shabbir, M. S. (2019). Investigating the impact of security factors in E-business and internet banking usage intention among Malaysians. *Industrial Engineering & Management Systems, 18(3), 501-510.*

Rao, P.B. (2024). A Study on Cyber Security Issues Affecting Online Banking and Transactions. *IJARIIE*. 9(6), 1655-1665.