WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

"A Study on the Impact of Cybercrime on the Banking Industry"

Srijal Tater[1], Dr. Batani Raghavendra Rao[2]

Under the Guidance of,
Dr. Batani Raghavendra Rao
Professor- Finance
Post-Graduate Student – MBA, CMS Business School, JAIN (Deemed-to-be University), Bengaluru – 560009

ACKNOWLEDGEMENT

I express my heartfelt appreciation to Professor **Dr. Batani Raghavendra Rao** for his invaluable guidance, mentorship, and unwavering support throughout the research process. His expertise and insights have been instrumental in shaping this work. I am deeply grateful for his time, expertise, and encouragement throughout.

ABSTRACT :

The report delves into the pervasive issue of cybercrime within the banking industry, examining its profound implications such as financial losses, reputational damage, and customer trust. Through an extensive literature review and a structured theoretical framework, the study identifies critical research gaps and proposes various hypotheses to explore the intricate relationship between cybercrime and banking. Employing a mixed-methods approach, combining secondary data analysis with primary surveys, the research gathers insights from 60 participants including banking professionals and students. Findings unveil a nuanced interplay between various factors and perceptions of cyber threats, revealing intriguing associations between cybersecurity awareness and the frequency of cybercrime attempts. Regional disparities in reported incidents underscore the complexity of the issue, with phishing, spoofing, malware, and SIM swap attacks emerging as prominent threats. The study underscores the need for tailored cybersecurity strategies within the banking sector, advocating for targeted education, awareness initiatives, and robust response mechanisms to mitigate evolving threats. This research sets the stage for future investigations to delve deeper into factors influencing cybersecurity perceptions and responses, paving the way for interventions aimed at bolstering the industry's resilience against cyber threats.

Keywords: Cybercrime, Banking Industry, Cybersecurity measures, Internet banking, Regulatory frameworks.

INTRODUCTION :

In our increasingly digital world, cybercrime has emerged as a significant threat to industries worldwide, with the banking sector particularly vulnerable. Cybercrime manifests in various forms, ranging from data breaches and phishing scams to ransomware attacks and insider threats. Each type poses unique risks and consequences for banks, their customers, and the financial ecosystem as a whole. Data breaches, for instance, compromise the confidentiality of sensitive information such as personal identifiers and financial records, leading to identity theft and fraud. Phishing scams exploit human vulnerabilities through deceptive emails or websites, tricking individuals into disclosing login credentials or financial details. Ransomware attacks encrypt critical data systems, extorting hefty sums from banks to regain access or prevent the public disclosure of stolen information. Insider threats, on the other hand, involve malicious actions by employees or trusted individuals within the bank, exploiting their access privileges to steal data or sabotage operations.

The impact of cybercrime on the banking industry extends far beyond financial losses, encompassing reputational damage, regulatory scrutiny, and erosion of customer trust. Incidents of cyber breaches can tarnish a bank's reputation and erode public confidence, leading to customer attrition and diminished market competitiveness. These activities pose severe risks to the security and stability of financial institutions, potentially undermining trust in the banking system and causing substantial financial losses for both institutions and customers alike. The banking industry stands at the forefront of technological innovation, leveraging digital platforms to streamline operations and enhance customer experiences.
Regulatory bodies impose stringent requirements on banks to safeguard customer data and maintain the integrity of financial systems, subjecting non-compliant institutions to fines and penalties.

Moreover, the evolving nature of cyber threats necessitates continuous investments in cybersecurity measures, imposing significant financial burdens on banks and diverting resources from core business activities. In this context, analysing the multifaceted impact of cybercrime in the banking industry is imperative for devising robust strategies to mitigate risks and safeguard against future threats. By understanding the types of cyber threats and their repercussions, banks can proactively enhance their cybersecurity posture, foster resilience, and uphold trust in the digital financial ecosystem.

REVIEW OF LITERATURE:

- **(More, Jadhav & Nalawade, 2015)** discusses that cybercrimes in India are increasing significantly, with offences such as social media, credit card fraud, phishing, virus, malware, denial of services, gambling, hacktivist, personal data breach, corporate data breach, and virtual currency. Males are more likely to commit these crimes, with Maharashtra ranking highest in state-wise cybercrimes. Most crimes are committed at Nationalized Bank Groups, causing significant money and data loss. To prevent cybercrimes, education on cybercrimes, punishments, and online banking precautions is crucial. Strong enforcement of rules and regulations is also necessary.
- **(Sabillion, Cano & Ruiz, 2016)** Cybercrime is a growing issue due to the rise of mobile devices, Wi-Fi networks, and the internet. To combat it, protection starts at personal levels and escalates to organizational, societal, corporate, national, military, and international levels. Integrating other fields like training, awareness, culture, laws, prosecution, and international cooperation is crucial.
- **(Goel, 2016)** explained that Indian customers are increasingly preferring online services due to convenience, cost-saving, and swift transactions. Financial institutions are offering attractive offers to boost cashless transactions. However, cyber security measures are being outpaced by the dynamic technological landscape and improved intruder expertise. Cybercrime has unique features, such as anonymity, global victim reach, and swift results. Insufficient awareness campaigns and traditional law enforcement policies are insufficient to address evolving cybercrimes.
- **(Ali, Ali, Surendran & Thomas, 2017)** recommends increasing the use of secure application software, developing robust systems to monitor fraudsters, enhancing user confidence, raising awareness about online threats, using strong passwords, and educating e-banking customers about the importance of a secure online banking environment. The survey results indicate that online banking users are not fully aware of the security threats they face from computer fraudsters and criminals. The lack of awareness allows criminals to access unauthorized customer information and carry out illegal activities.
- **(Iqbal & Beigh, 2017)** The rapid growth of internet use, especially in India, has led to a surge in cybercrime, making the country vulnerable. Cyberspace is free-flowing and unguarded, making it difficult to deter such crimes. India has engaged in bilateral agreements with Russia, the US, and Israel, but these have limited scope and are ineffective. India needs a multilateral treaty to harmonize its laws and promote international cooperation in combating cybercrimes. The Council of Europe's Budapest Convention on Cybercrime could be a valuable international treaty.
- **(Mohapatra, 2018)** pointed that RBI recently addressed all banks in India a statement urging them to update their security standards and deploy a revolutionary cyber security system in accordance with the RBI's guidelines. This requirement is common, and it is customary for the governing body of the world's central banks to introduce new and enhanced regulatory compliance legislation. While all of this may appear rudimentary on the surface, it does provide one reason to consider and reflect on the grounds for such a mandate.
- **(Jain & Gupta, 2020)** expresses that cybercrime is a major challenge for India and international law enforcement, involving drug trafficking, people smuggling, terrorism, and money laundering. Digital evidence will become more common in traditional crimes, necessitating new partnerships, forensic methodologies, and responses to ensure safety and security on the internet. Innovative responses, such as cyber cops, courts, and judges, may be needed to overcome jurisdictional issues. Cyber law in India combines Contract, Intellectual property, Data protection, and privacy laws to protect information, software, information security, e-commerce, and monetary transactions.
- **(Shah, 2020)** study reveals a higher share of private and foreign bank crime related to online banking, ATM cards, and other digital transactions. Cybercrime is a global concern, with most crimes resulting from hacking and identity theft. Banks can only partially prevent these crimes, as they cannot stop users from using online banking and check their computers for malware. The study also shows that customers are not alert and have limited knowledge of cybercrimes. In India, cybercrimes are increasing, with most focusing on nationalized banks. Banks must educate users about cybercrimes and take precautions to safeguard their computers and personal data.
- **(Sethi, 2021)** Cyber security is a complex issue involving various fields and disciplines. While technological measures are important, it's not primarily a technological problem. The problem's solutions are both technical and nontechnical. Solutions include specialized banking software development, secure socket layers (SSL), MFA, OTP, SSO, and SFTP. The problem will never be completely resolved, but solutions are limited in scope and endurance.
- **(Singh, 2021)** explores the concept of e-banking and the impact of cyber-crimes on the banking sector. Information Technology has become the backbone of the banking system, supporting challenges and requirements. However, it also has negative impacts, such as phishing, hacking, forgery, and cheating. To prevent cyber-crime, authentication, identification, and verification techniques must be implemented. The National Crime Records Bureau found a significant increase in cyber-crimes in India in the past three years. The study suggests that while eliminating cybercrime is not a feasible task, regular checks on banking activities and transactions can help.
- **(George & Nagadeepa, 2023)** explores the increasing impact of cybercrimes in electronic financing, primarily resulting from hacking and identity theft. It emphasizes the need for precautions such as strong passwords, two-factor authentication, updated software, and monitoring accounts for unusual behaviour. Businesses should invest in security measures like firewalls and antivirus software. The study also suggests a systematic approach to minimizing cybercrime impacts.
- **(Harisha, Mishra & Singh, 2023**) discusses cyber forensics, Indian cyber laws, and various models of investigation. Cybercriminals often misuse technology for their goals, and most cybersecurity professionals approach cybercrime reactively & suggests using machine learning techniques to train security systems to identify and block malicious traffic. Challenges include a globally accepted definition of cybercrime, inadequate access to investigators, and complex extradition processes.

RESEARCH METHODOLOGY:

3.1 Objectives of the Study

1. Assess the frequency and types of cybercrimes targeting the banking sector.
2. Investigate the financial losses incurred by banks due to cybercrimes over a specified period.
3. Evaluate the effectiveness of current cybersecurity measures and protocols implemented by banks.
4. Analyse the efficiency of regulatory frameworks and compliance standards governing cybersecurity in the banking industry.
5. Identify the most vulnerable areas within banks' infrastructure and operations to cyber threats.

3.2 Problem Statement

The banking industry faces a complex array of challenges stemming from the pervasive threat of cybercrime, necessitating a deeper understanding of its multifaceted impacts and underlying vulnerabilities. Cyberattacks not only result in significant financial losses for banks but also inflict reputational damage, erode customer trust, and impose burdensome regulatory compliance requirements. Despite the implementation of cybersecurity measures, banking systems remain susceptible to evolving cyber threats, highlighting the need to assess the efficacy of current approaches in safeguarding against cybercrimes.

3.3 Data Collection & Methods

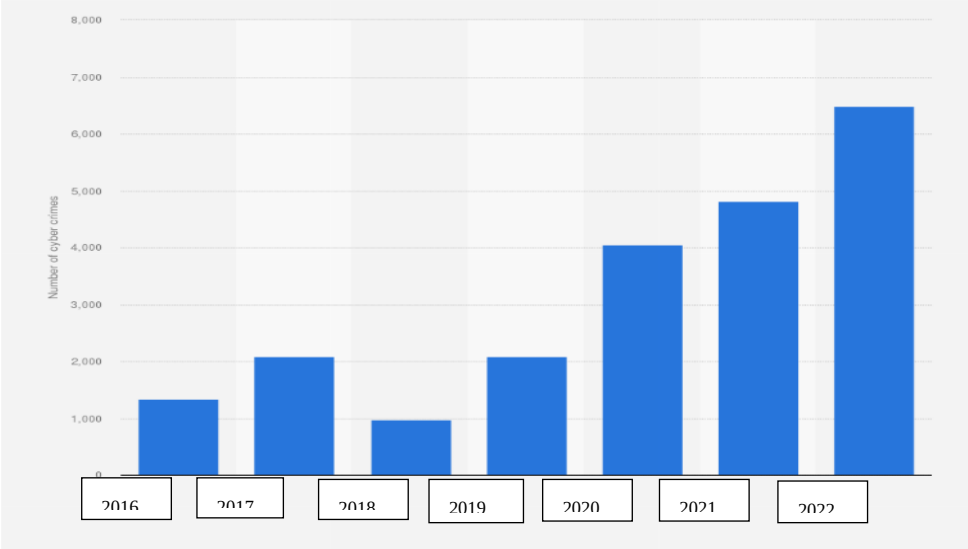
The study integrates both secondary data analysis and primary survey to comprehensively investigate cybercrime in the banking sector. Secondary data will be collected from credible sources such as academic journals and industry reports, providing foundational insights into existing literature and forming hypotheses for the survey. The survey will involve structured distributed among a sample of 60 individuals, including banking professionals and students. Sampling techniques such as random sampling will be used and data will be analysed using Chi- test in SPSS.

3.4 Scope of the Study

This study aims to provide a comprehensive analysis of the impact of cybercrime on the banking industry, focusing on prevalent forms such as phishing attacks, malware infections, spoofing, and others. By examining the immediate and long-term consequences of cybercrime on banks, including financial losses, reputational damage, and regulatory implications, the study seeks to deepen understanding of the challenges faced by the banking sector in combating cyber threats. Additionally, the research will evaluate the effectiveness of existing cybersecurity measures employed by banks and assess the role of regulatory standards in promoting cybersecurity resilience.

DATA ANALYSIS & INTERPRETATION:

Fig 1.1: Online banking cybercrimes across India



source: Statista2024

In 2022, there were over 6.4 thousand cases of online banking frauds reported across India. This was a big increase in the number of banking fraud cases than the previous year. Telangana had the highest cases of about 3,223 banking frauds that year.

Fig 1.2: Cybercrime reported to NCCRP

source: https://timesofindia.indiatimes.com/

Between January 1, 2020, and May 15, 2023, Gujaratis made a total of 1.59 lakh applications related to cybercrime on the National Cyber Crime Reporting Portal (NCCRP) or helpline number 1930. It comes to 5,585 applications per month on an average, 186 applications per day and average one application every 7.5 minutes.

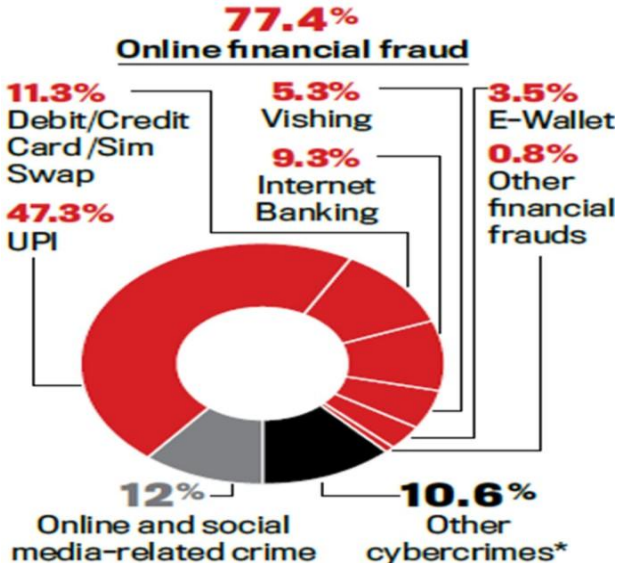
Fig 1.3: Frauds reported in banking operations

	Number of frauds	Amount involved (in ₹ cr)
2020-2021	7,263	118,417
2021-2022	9,053	45,598
2022-2023	13,576	26,632
2022-2023*	5,396	17,685
2023-2024*	14,483	2,642

source: https://www.business-standard.com/

The number of frauds reported by banks has gone up from 7,263 in 2020-21 to 14, 483 in 2023-24. The amount involved in these frauds has seen a significant decline from Rs 1,18,417 crore to Rs 2,642 crore during the same period.

Fig 1.4: Cybercrimes offences trend from 2020 to 2023



source: https://www.indiatoday.in/

Fig 1.5: Cybercrime types with victim counts

2022 CRIME TYPES

By Victim Count

Crime Type	*Victims*	*Crime Type*	*Victims*
Phishing	300,497	Government Impersonation	11,554
Personal Data Breach	58,859	Advanced Fee	11,264
Non-Payment/Non-Delivery	51,679	Other	9,966
Extortion	39,416	Overpayment	6,183
Tech Support	32,538	Lottery/Sweepstakes/Inheritance	5,650
Investment	30,529	Data Breach	2,795
Identity Theft	27,922	Crimes Against Children	2,587
Credit Card/Check Fraud	22,985	Ransomware	2,385
BEC	21,832	Threats of Violence	2,224
Spoofing	20,649	IPR/Copyright/Counterfeit	2,183
Confidence/Romance	19,021	SIM Swap	2,026
Employment	14,946	Malware	762
Harassment/Stalking	11,779	Botnet	568
Real Estate	11,727		

Source: https://www.techopedia.com/

Fig 1.6: Hypothesis-1 testing by Chi-test

Null hypothesis (H0): There is no significant association between a respondent's familiarity with cybersecurity regulations and their rating of the effectiveness of their bank's cybersecurity measures.

Alternative hypothesis (H1): There is significant association between a respondent's familiarity with cybersecurity regulations and their rating of the effectiveness of their bank's cybersecurity measures.

Are you familiar with the regulatory frameworks and compliance standards governing cybersecurity in the banking industry? * Please rate the effectiveness of the following cybersecurity measures currently implemented by your bank. Crosstabulation

			Please rate the effectiveness of the following cybersecurity measures currently implemented by your bank.					
			1	2	3	4	5	Total
Are you familiar with the regulatory frameworks and compliance standards governing cybersecurity in the banking industry?	No	Count	1	0	2	7	2	12
		Expected Count	.6	.6	2.4	7.8	.6	12.0
	Yes	Count	2	3	10	32	1	48
		Expected Count	2.4	2.4	9.6	31.2	2.4	48.0
Total		Count	3	3	12	39	3	60
		Expected Count	3.0	3.0	12.0	39.0	3.0	60.0

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	5.353[a]	4	.253
Likelihood Ratio	4.889	4	.299
N of Valid Cases	60		

a. 7 cells (70.0%) have expected count less than 5. The minimum expected count is .60.

The chi-square test statistic is 5.353 with 4 degrees of freedom. The asymptotic significance (2-sided) is 0.253. Both p-values are above the conventional threshold of 0.05. So, we accept the null hypothesis.

Fig 1.7: Hypothesis-2 testing by Chi-test

Null hypothesis (H0): There is no significant association between the frequency of financial losses and its impact on stability & trustworthiness of the banking sector.

Alternative hypothesis (H1): There is significant association between the frequency of financial losses and its impact on stability & trustworthiness of the banking sector.

How often do you believe your bank has experienced financial losses due to cybercrime in the past? * How do cybercrimes impact the stability and trustworthiness of the banking sector? Crosstabulation

			How do cybercrimes impact the stability and trustworthiness of the banking sector?					
			High	Low	Moderately	Very High	Very Low	Total
How often do you believe your bank has experienced financial losses due to cybercrime in the past?	Never	Count	6	1	1	1	1	10
		Expected Count	5.7	.3	1.7	2.0	.3	10.0
	Often	Count	3	0	3	1	0	7
		Expected Count	4.0	.2	1.2	1.4	.2	7.0
	Rarely	Count	15	1	5	4	0	25
		Expected Count	14.2	.8	4.2	5.0	.8	25.0
	Sometimes	Count	10	0	1	4	0	15
		Expected Count	8.5	.5	2.5	3.0	.5	15.0
	Very Often	Count	0	0	0	2	1	3
		Expected Count	1.7	.1	.5	.6	.1	3.0
Total		Count	34	2	10	12	2	60
		Expected Count	34.0	2.0	10.0	12.0	2.0	60.0

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	24.597[a]	16	.077
Likelihood Ratio	21.248	16	.169
N of Valid Cases	60		

a. 21 cells (84.0%) have expected count less than 5. The minimum expected count is .10.

The chi-square test statistic is 24.597 with 16 degrees of freedom. The asymptotic significance (2-sided) is 0.077. Because the significance level in this case is greater than 0.05, we accept the null hypothesis.

FINDINGS & DISCUSSION :

Between January 1, 2020, and May 15, 2023, the national ratio was found to be 1.9% as 43,022 FIRs were filed based on 22.57 lakh applications. In 2022, there were over 6.4 thousand cases of online banking frauds reported across India. This was a big increase in the number of banking fraud cases than the previous year. During and after lockdowns, a steep rise in digital transactions gave the spammers and online frauds an opportunity to fleece the persons who were not digital savvy. The fraudsters are using new techniques to cheat customers. These include phishing, malware being designed to extract and copy data from the infected device of a bank customer, phishing and SIM swap.

The Bureau report showed of the total reported digital payment frauds in May 2022, as many as 55% were related to UPI transactions, half of which were of less than Rs 10,000 in ticket size. Advanced monitoring mechanisms is needed to be installed by banks for real-time detection and prevention of digital frauds. Increased digitalization and reliance on internet banking and the ease of switching mobile network operators make customers more vulnerable to fraud, especially through methods like ATM hacking and UPI usage. This rise can be attributed to increased technology exposure among people who may not be fully aware of the risks involved. Hackers exploit the lack of awareness by impersonating bank officials and tricking customers into revealing personal data, leveraging spam emails and fake network swap requests to obtain sensitive information like OTPs, ultimately leading to unauthorized access to bank accounts.

The common areas of fraud in banking operations included advances, forex transactions, deposits, and operations involving card or internet transactions. In number terms, H1FY24 saw credit and internet-related transactions as the most common types of fraud. The operational impact associated with mitigating and addressing fraud can be extensive. Fraud is often viewed in the context of the bottom line. However, among the most underrecognized consequences is the near- and long-term impact it can have on topline revenue. There is often an opportunity cost associated with fraud prevention.

However, the Chi- test analysis results find no significant relationship between familiarity with cybersecurity frameworks and ratings of cybersecurity measures & in between financial losses & their impact on stability & trustworthiness of customers. Most respondents were familiar with cybersecurity regulations in banking, but that does not significantly impact their perceptions of the effectiveness of cybersecurity measures implemented by their banks. Which implies that familiarity does not influence individuals' perceptions of the effectiveness of cybersecurity measures. Overall, respondents tend to view these measures positively, with a majority rating them as relatively effective. Also, based on survey, respondents generally believe their banks have rarely experienced financial losses due to cybercrime indicating that this belief is not significantly related to their perceptions of how cybercrimes impact the stability and trustworthiness of the banking sector.

CONCLUSION

The findings reveal a concerning trend of rising cybercrimes targeting banks. The period between January 2020 and May 2023 saw a significant number of cybercrime incidents, with phishing, malware attacks, and SIM swaps being prevalent methods. This rise coincides with the increased adoption of digital transactions, particularly during lockdowns, highlighting the vulnerability of individuals unfamiliar with online security practices. The study also underscores the financial losses incurred by banks due to cybercrime. Notably, a substantial portion of these losses stemmed from UPI transactions, often involving smaller amounts. This emphasizes the need for robust monitoring mechanisms by banks to proactively detect and prevent such fraudulent activities.

Additionally, the research identified the operational impact of cybercrime, extending beyond financial losses and potentially affecting customer trust and top-line revenue. The study highlights the importance of not only implementing robust cybersecurity protocols but also actively educating customers about online security practices underlining the need for targeted security measures to address these specific vulnerabilities.

Cybercrime poses a significant threat to the banking sector. While existing cybersecurity measures offer a layer of protection, banks have implemented various cybersecurity measures, there is room for improvement, particularly in addressing emerging cyber threats and vulnerabilities. Continuous improvement, evaluation and enhancement of regulatory frameworks, coupled with increased awareness and education among customers, are essential to mitigate the risks posed by cybercrimes and ensure the stability and trustworthiness of the banking sector. Regulatory frameworks also require close scrutiny to ensure their effectiveness in mitigating cyber threats. By acknowledging these challenges and implementing comprehensive solutions, the banking industry can safeguard itself and maintain customer trust in the digital age.

REFERENCES :

1. Goel, S. (2016). Cyber-Crime: A growing threat to Indian banking sector. *International Journal of Science Technology and Management*, *5*(12), 552-559.
2. Singh, N. (2021). *Cybercrime of Banking sector in India, Challenges and remedies* (Doctoral dissertation).
3. George, S., & Nagadeepa, C. (2023). A STUDY ON THE RISING IMPACTS OF CYBERCRIMES IN ELECTRONIC FINANCING. *Role of Management and Business Practices for Sustainable Development*, 63.
4. More, D. M. M., & Nalawade, M. P. J. D. K. (2015). Online banking and cyber-attacks: the current scenario. *International Journal of Advanced Research in Computer Science and Software Engineering Research Paper*.
5. Jain, A., & Gupta, N. (2020). Cyber crime. *National Journal of Cyber Security Law*, *2*(2), 152-158.
6. Shah, I. (2020). Analysis of Cyber Crime in Banking Sector.
7. Iqbal, J., & Beigh, B. M. (2017). Cybercrime in India: trends and challenges. *International Journal of Innovations & Advancement in Computer Science*, *6*(12), 187-196.
8. Sethi, N. (2021). Cyber security analysis in banking sector. International Journal of Recent Scientific Research, 12(7), 12345-12349.
9. Harisha, A., Mishra, A., & Singh, C. (Eds.). (2023). Advancements in Cybercrime Investigation and Digital Forensics (1st ed.). Apple Academic Press. https://doi.org/10.1201/9781003369479
10. Mohapatra; K. (2018). effective operational risk management Cybersecurity vulnerability in Indian banks. Cybersecurity Framework in Banks. Retrieved from: https://financialit.net/sites/default/files/customerxps_white_paper_cybersecurity_vulnerability_in_indian_banks_1.pdf
11. Sabillon, R., Cano, J. J., & Serra Ruiz, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security, 2016, 4 (6)*.
12. Ali, L., Ali, F., Surendran, P., & Thomas, B. (2017). The effects of cyber threats on customer's behaviour in e-banking services. *International Journal of e-Education, e-Business, e-Management and e-Learning*, *7*(1), 70-78.
13. Statista. (2023, December 19). India: number of cyber crimes related to online banking 2022 [Statistic]. Retrieved April 12, 2024, from https://www.statista.com/statistics/875887/india-number-of-cyber-crimes-related-to-online-banking/
14. Singh, S. (2024, January 4). From the India Today archives: 2023-online fraud, a raging menace [Amp]. India Today. https://www.indiatoday.in/amp/india-today-insight/story/from-the-india-today-archives-2023-online-fraud-a-raging-menace-2484367-2024-01-04
15. McKee, J. (2020, November 22). Unpacking the overall impact of fraud. Forbes. https://www.forbes.com/sites/jordanmckee/2020/11/22/unpacking-the-overall-impact-of-fraud/?sh=7de025427891
16. Press Trust of India. (2023, December 27). Total amount of frauds reported by banks declines to six-year low: RBI [Amp]. Business Standard. https://www.business-standard.com/amp/finance/news/total-amount-of-frauds-reported-by-banks-declines-to-six-year-low-rbi-123122701013_1.html
17. Shah, M. (2023, April 18). Every 7.5 mins, a cybercrime reported from Gujarat [Amp]. The Times of India. https://timesofindia.indiatimes.com/city/ahmedabad/every-7-5-mins-a-cybercrime-reported-from-gujarat/amp_articleshow/101469822.cms
18. Phishing statistics. (n.d.). Techopedia. https://www.techopedia.com/phishing-statistics