Chapter 19

Cyber Crime: A Constant Threat to Indian Banking Sector

Shashank Bhardwaj *

Abstract The Indian banking industry has kept up with developing trends and major operational changes as a result of technological improvements. Banks are now among the largest benefactors of the IT revolution as a result of the enormous potential that the call for expansion has provided this institution. The exponential growth of online transactions. Banking Sector now has shifted its focus on adapting latest emerging technologies i.e., NEFT, RTGS, ECS, Mobile banking, UPI, Blockchain, Fintech, Cloud computing, Artificial Intelligence, Big Data and Virtual Reality which is the evidence of the fact that how technology has upgraded the financial system in the Indian banking sector (Mittal, 2020; Tiwari et al.,2021).

However, opportunities also carry risks, and success has its own unique set of challenges (Mittal & Gautam 2023). In the lexicon of criminal language, the term "cybercrime" is relatively new; it gained traction mostly in the late 1990s when technology was brought to the financial sector. The technological aspects of cybercrimes, their effects on the financial sector, and the challenges and fallout they create are the main topics of this research paper. Additionally, it highlights the need for stronger, more reliable security against upcoming cyberattacks.

Thus, as computer and internet technology quickly advanced, new types of global crimes known the term "Cyber Crimes" has developed. The nature and pattern of cybercrime occurrences have evolved over time to become increasingly complicated and sophisticated. Since the

*Sharda School of Business Studies, Sharda University, Greater Noida-201310, India. *Corresponding Author ✉ shashank.bhardwaj@sharda.ac.in

Prabhat Mittal and Rajeev Bansal (eds), Social Development and Governance: Innovations in Education, Technology & Management (ISBN: 978-81-966500-9-4)
https://doi.org/10.48001/978-81-966500-9-4_19

last decade, banks and other financial institutions have continued to be targeted by cybercriminals. There is little prospect that this will change anytime soon; most cybercriminal operations are still primarily motivated by financial gain. The technological features of numerous cybercrimes affecting financial units and their effects are the main subject of this article. It further analyses the danger vectors that facilitate these crimes and develops countermeasures to assist fend off subsequent cyberattacks in order to better prevent such assaults in the future for greater security.

Keywords Identity theft, e- Banking, Cybercrime and Fraud Detection.

19.1 Introduction

According to internetlivestats.com, 46.1% of the world's population is currently online, indicating that the online world is expanding quickly. (as on July 1, 2016). A notable occurrence of this phenomenon occurred in India, where the percentage of online users has significantly increased over the past three years (18% in 2014, 27% in 2015, and 34.8% in 2016), (as on July 1, 2016). (Mittal , 2020) Today, internet usage is not just for geeky technical purposes; rather, every second person is taking advantage of the easy availability and accessibility of the internet for everyday needs like banking, e-Online services are in high demand, but due to multiple obtrusive actors generally known as "Cyber-Crime," it appears to be a difficult issue to provide balanced security and convenience (Rao, 2019; Gupta et al., 2023).

Goel (2016) analyzed that due to the ease, affordability, and speed of online transactions, Indian consumers are rapidly favoring online services. Furthermore, financial institutions are making clients more alluring incentives in an effort to increase the number of cashless transactions because they have relatively lower operating expenses.

The banking industry in India cannot stop transactions that are conducted electronically, and is facing the outcomes of cybercrime which is a more serious offence than traditional crimes. To combat this issue, victims can submit their cases to the closest police station as well as the cyber-fraud council inside banks. To prevent these problems, lawmakers should closely supervise the way banks operate, enforce laws strictly to prevent wrongdoings of this kind, and

encourage banks to regularly inform their clientele about the dangers of cybercrime.

Sarkar et al. (1998) in a study highlights that a range of email-borne viruses, spyware, adware, Trojan horses, phishing attacks, directory harvest assaults, denial-of-service attacks, and other dangers combine to attack businesses and clients despite the fact that it is difficult to conceive a workplace without access to the internet. This essay makes an effort to review phishing, a hazard to Internet-based business transactions that is continually expanding and changing. We'll talk about several phishing techniques like vishing, spear phishing, pharming, key loggers, malware, web Trojans, and more. This article also presents the most recent phishing analyses produced by the Korean Internet Security Center and the Anti-Phishing Working Group (APWG).

Despite a number of highly publicized cyberattacks in recent years, very few businesses have taken the required precautions to isolate industrial control systems and critical data and to reduce the harm an attack can cause. Dealing with technological challenges, which are usually simple and tactical, is only one aspect of security. The key strategic challenge is governance: coordinating efforts across departments to make sure that information technology, physical security, and legal requirements all operate together (Asif et al., 2023).

19.2 Finding of the Study

1. Hacking and identity theft are the main causes of cybercrimes in this industry.
2. Due to the fact that banks hold all of the reserves in the form of currency, banks are frequently attacked.
3. Customers' security is much at stake because of how easy it has become to hack into people's personal information.
4. Fraud detection software is frequently either outdated or takes a very lengthy time to operate.

5. These crimes, especially those involving the financial industry, are not specifically covered by law.

19.3 Discussion & Suggestions

- Since there is no specific law enforcement, the principal effects of these crimes are frequently unresolved, hence legislation must be implemented to stop this type of threat.
- The law enforcement should be highly strict and provide regular updates in order to maintain track of such offences.
- It should be possible to resolve these conflicts, handle public complaints, and promote public trust through the use of fast track mobile courts.
- With the aid of Big Data Banks, the government should also maintain tabs on the actions taking place within the operating network.
- To lessen the effects of these problems and punish the assailants, severe punishments and penalties must be used.
- Awareness campaigns should be launched to alert the public of the current situation and impending dangers.
- Instead of only sending these situations to the banks, the public should report them to the Cyber Crime Branch in order to ensure swift and rigorous action.

19.4 Conclusion

In this research paper, researcher investigated the new types of crimes in the chosen area of study. The criminals of modern day try to carry out these new crimes using computers and the Internet by abusing cyberspace. According to estimates, cash is used in 95% of transactions in India, but as the use of computers, smartphones, and internet access grows, Indians are

increasingly using digital channels for their financial needs. Because of this, cybercrime is becoming a bigger problem.

The RBI defines bank fraud as any transaction involving deceit, carelessness, misappropriation of funds, or the use of false documents. The RBI stated that "increased audacious attacks by organized gangs with or without backing from state players have come to light," in addition to straightforward attacks utilizing phishing, vishing, and social engineering. The RBI advised banks to purchase preventative software and regularly review the risks at hand, not just for internal operations but also for the third parties the lenders use. If executed properly, this can be seen as a brilliant approach because hackers frequently access the personal information of customers and/or banks, depending on the situation. They frequently come up with creative ways to perpetrate these crimes, so before anyone can figure. The speed and intensity of these fraudulent transactions, which happen in a matter of seconds, is what went wrong; the harm has already been done. The time has come to take into account how such crimes affect society from a fair standpoint in order to prevent online criminals from getting away with their crimes. Cybercrime is a common form of international crime.

Since the financial security of the banking industry determines the financial security and safety of our country's assets as a whole, it is imperative that we acknowledge the urgency of the situation and take a strong stand against cybercrime. This is because the jurisdiction in this area is complicated and still unclear. India cannot jeopardize the security of such a crucial plant at its level of development. We will be able to accelerate the rate of overall growth and development and get closer to improvement if we are able to stop these attacks, one by one, shortly in the future.

References

Mittal, P. (2020, November). A multi-criterion decision analysis based on PCA for analyzing the digital technology skills in the effectiveness of government services. In 2020 International Conference on Decision Aid Sciences and Application (DASA) (pp. 490-494). IEEE.

Tiwari, S., Bharadwaj, S., & Joshi, S. (2021). A study of impact of cloud computing and artificial

intelligence on banking services, profitability and operational benefits. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(6), 1617-1627.

Mittal,5.Mittal, P., & Gautam, S. (2023). Logistic Regression and Predictive Analysis for AI Strategies in Public Services. technology, 18, 19.

.Mittal, P. (2020, October). Impact of digital capabilities and technology skills on effectiveness of government in public services. In 2020 International Conference on Data Analytics for Business and Industry: Way Towards a Sustainable Economy (ICDABI) (pp. 1-5). IEEE.

Harshita Singh Rao (2019)," cybercrime in banking sector", International Journal of Research – Granthaalayah, Vol- 7(1) PP.148.

Gupta, S., & Tiwari, S. (2023). New Technological Advancements and Its Impact on Healthcare System. VEETHIKA-An International Interdisciplinary Research Journal, 9(1), 27-32.

Goel, S. (2016). Cyber Crime: A Growing threat to Indian Banking Sector.International Journal of Science Technology and Management,5(12), 552-559.

Asif, M., Khan, M. N., Tiwari, S., Wani, S. K., & Alam, F. (2023). The impact of fintech and digital financial services on financial inclusion in India. Journal of Risk and Financial Management, 16(2), 122.

Kesharwani, S., Sarkar, M. P., & Oberoi, S. (2019). Growing threat of cybercrime in Indian banking sector. Cybernetics, 1(4), 19-22

Bhaumik, S. K., & Piesse, J. (2008). Does lending behavior of banks in emerging economies vary by ownership? Evidence from the Indian banking sector. Economic Systems, 32(2), 177-196.

Singh, C., Pattanayak, D., Dixit, D., Antony, K., Agarwala, M., Kant, R.,& Mathur, V. (2016). Frauds in the Indian banking industry. IIM Bangalore Research Paper, (505).

Chakraborty, M. (2015). Risk analysis and management in Indian banking sector: An overview. International Journal of Informative & Futuristic Research, 2(7), 2133-2143.

Mayur Abhyankar, Ketan Patil (2019),"A study of Frauds in Banking Industry", Indian Journal of Applied Research, Vol- 9(5).

Swain, S. C. (2021). Cybersecurity Threats and Technology Adoption in the Indian Banking

Sector: A Study of Retail Banking Customers of Bhubaneswar. In Strategies for E-Service, E-Governance, and Cybersecurity (pp. 51-65). Apple Academic Press.

Koju, L., Koju, R., & Wang, S. (2018). Does banking management affect credit risk? Evidence from the Indian banking system. International Journal of Financial Studies, 6(3), 67.

Sinha, A. (2012). Indian Banking—Journey into the Future. Reserve Bank of India Monthly Bulletin, 2, 43-49.

Kamath, K. V., Kohli, S. S., Shenoy, P. S., Kumar, R., Nayak, R. M., Kuppuswamy, P. T., & Ravichandran, N. (2003). Indian banking sector: Challenges and opportunities. Vikalpa, 28(3), 83-100.

Sarkar, J., Sarkar, S., & Bhaumik, S. K. (1998). Does ownership always matter?—Evidence from the Indian banking industry. Journal of comparative economics, 26(2), 262-281.

Khan, M. A., & Ahmad, W. (2022). Fresh evidence on the relationship between market power and default risk of Indian banks. Finance Research Letters, 46, 102360.