Journal of Advances and Scholarly Researches in Allied Education
Vol. 19, Issue No. 6, December-2022, ISSN 2230-7540

An Overview of Indian Perspective on Cyber Crime in Banking Sector

Renu Vijaywargia[1]*, Dr. Anil Kumar Jeph[2]

[1] Research Scholar, Raj Rishi Bhartrihari Matsya University,Alwar-301001, Rajasthan

[2] Professor, Govt. Law College, Raj Rishi Bhartrihari Matsya University,Alwar-301001, Rajasthan

Abstract - Financial crime in India is the focus of this research. It provides an overview of the issues currently confronting the financial sector, as well as potential solutions. Cybercriminals often aim their attacks at financial institutions. Gordon Snow, assistant director of the Cyber Division of the Federal Bureau of Investigation, expects cyber assaults on financial institutions to increase in frequency and sophistication. The rise of e-commerce presents several new entry points for cybercriminals.

Keywords - Bank, Cyber Crime, Economic sector, Information and Communication Technology

----------X----------

INTRODUCTION

Economic crime is a major issue in India, as shown by the findings of the 2011 Global Economic Crime Survey. The number of Indians who use the internet has exploded in recent years. The results of a recent survey conducted by the Telecom Regulatory Authority of India (TRAI)[1], At this time, there are 354 million internet users worldwide.

The prevalence and sophistication of online misbehaviour have increased over time and across many different mediums. In the last decade, hackers' primary objectives have been financial institutions like banks and nonprofits. Up until recently, most cybercrime was motivated by financial gain, but there is hope that this is changing.[2]

Financial crime is a big problem that the international community is trying to solve right now. The economy of the vast majority of countries have tanked as a result. These days, fraud and fraudulent practises are the only real threats to the financial sector. (p. 140) According to (Folami, 2011). There has been an increase in reporting on cyber risk as a major threat to financial institutions like banks.

The most typical reasons for a cyber attack include:

- A toxic combination occurs when a person changes jobs but keeps the same level of access to the system they were previously responsible for.
- Sensitive information is at risk of cyber assaults due to poor data management.
- The prevalence of social media, mobile devices, and network access from distant locations all contribute to a rise in the likelihood of cyber security breaches.
- Inadequate knowledge of cyber risks and mitigation strategies among banking industry executives and regulatory bodies.

When it comes to the lending process, a high degree of digitization is marked by scalability, an emphasis on intangible information, and significantly increased levels of user engagement. Legally speaking, DLAs/ LSPs who arbitrate between many lenders and borrowers are in a grey area under the IT Act of 2000. An intermediary is defined as follows in Section 2(1)(w) of the Act:

Telecom companies, network providers, ISPs, web hosts, search engines, payment sites, auction sites, marketplaces, and cyber cafes are just some of the many examples of service providers that fall under the umbrella term "intermediary" when discussing specific types of digital documents.

A victim of economic crime might be anybody. Its influence spans the whole planet. No company or sector is safe. Despite fraud being a major problem for businesses, the number of respondents who did not know whether or not their organisation had been a victim of economic crime in the previous year rose

[1] https://www.trai.gov.in/release-publication/reports/survey-reports

[2] https://www.legalserviceindia.com/legal/article-3073-cyber-frauds-in-the-indian-banking-industry.html retrieved on 20 December 2022

from 6% in 2009 to 10% in 2011. The issue of poor knowledge is likely exacerbated by the infrequency with which fraud risk assessments are undertaken. Despite the clear benefits, one-third of respondents said they never do a fraud risk assessment. As a consequence of this trend, more companies are vulnerable to fraud. Loss of market share, decreases in employee morale, and other indirect costs are all possible outcomes of economic crime. Companies now face a public that is less tolerant of unethical behaviour and must change accordingly.

make sure they are doing everything they can to gain and keep people's trust. In today's environment, digital resources are essential for the vast majority of people and businesses. As a result, they open themselves up to attacks from hackers all around the world. This research examines the scope and effect of this new kind of economic crime on enterprises throughout the world against the backdrop of data loss and theft, computer viruses, and hackers. The economic impact of cybercrime is significant enough to rank in the top four. Many people (58% to be exact) believe that IT is especially prone to cybercrime. Respondents estimated that their employers monitored their internal and external internet conversations and activities at a rate of 96%. Eighty percent of Indian respondents stated they think the threat of cyber crime originates from inside India or a combination of sources both within and outside the country. Sixty-three percent of people who were surveyed indicated they had no way to get forensic technology equipment. Thirty-one percent of those polled said they had received no cyber security training in the last year. There has been a steady increase from 20% in 2007 to 68% in 2011 in the rate of theft of another's property, the most prevalent kind of economic crime. Almost two-thirds of respondents found out that the offenders were employed by the company. Men between the ages of 31 and 40 with a bachelor's degree made up the vast majority of con artists. In a survey, 80% of employees stated the organisation had fired the offender and 51% said they would never work with an outsider who participated in fraudulent actions again. Despite growing assurance in their risk management systems, the majority of fraud (35% in one study) is still uncovered by chance.[3]

Financial loss due to cyber crimes[4]

Year	Extent of loss (Rs crore)	Amount involved (Rs crore)
2019-2020	58.61	194.39
2020-2021	63.40	195.80
2021-2022	68.73	197.50

Fraud and its connected activities are prohibited under and punished by a number of Indian laws. Section 25 of the Indian Penal Code tries to define "fraud" by stating that "there can be no fraud unless there is an intention to defraud." There are several situations and goals that call for the use of deceit, like as.

- To behave in a manner that violates a man's legal rights, such as by stealing from him or intruding on his property.
- Keeping someone from getting their due money by making up false allegations or being dishonest in any other way.
- To illegally prevent someone from making use of their property.
- Whenever the context calls for "fraud," "intent to defraud," "expose," or "actual" or "potential" harm to someone.
- In every instance of fraud, the perpetrator's primary motivation is to increase his own personal gain.

Number of bank fraud cases across India between from financial year 2009 to 2022

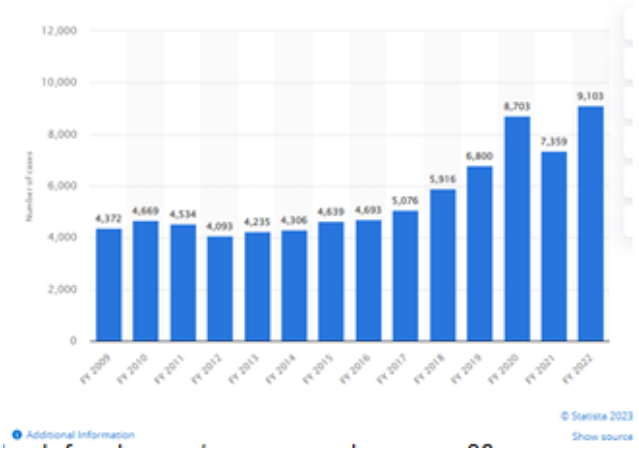


Figure 1- Number of bank fraud cases across India between from financial year 2009 to 2022

(Source: https://www.statista.com/statistics/1012729/india-number-of-bank-fraud-cases/ accessed on 26 February 2023)

The incidence of fraud in India is shown in Figure 1 from 2009 to 2022. About 9,103 incidents of bank fraud were reported to the Reserve Bank of India (RBI) in 2022. This reversed a decade-long

[3] Nainta, R.P., "Banking System Fraud and Legal Control", Deep and Deep Publications, (2005), New Delhi-110027,P-44

[4] https://timesofindia.indiatimes.com/business/india-business/cyber-crime-losses-rise-to-rs-63-crore-in-fy20-21- govt/articleshow/90532711.cms

downward trend and was an improvement over the prior year. Indian bank fraud losses fell from 1.38 trillion rupees to 604 billion rupees between 2010 and 2017.[5]

The fraudulent use of the Internet is covered here. Such scams include both dishonesty (or the desire to deceive) and actual or prospective injury to the victim(s), making them fraudulent. Every con has the same end result: the perpetrators gain while the victims lose.

Books used in the CBI In what has been dubbed India's largest financial scam, DHFL[6] Sponsors had a role. The FIR alleges that the defendants plotted to defraud 17 banks. The complaint alleges that Kapil Wadhawan, the chairman of DHFL, and others committed fraud in order to get funding from banks totaling 42,871 crore rupees. The total amount of money stolen from banks as a result of this crime and embezzlement was 34,615 crore rupees. The company was sold to Piramal Enterprises in September of last year after bankruptcy court procedures. A KPMG forensic audit found that "large amounts were disbursed as loans & advances by the borrower company to a number of interconnected entities and individuals with commonalities to DHFL Promoter Entities," with the money being used to buy shares and debentures in the company."[7]

Famous cases in India [8]

1. Vijay Mallya Fraud case[9]
2. Punjab National Bank scam[10]
3. ABG Shipyard fraud case[11]
4. Andhra Bank fraud[12]
5. Rotomac Pen Scam[13]
6. Videocon Case fraud[14]

KPMG[15] “An example of such a summary may be seen in the "Issue Digest: Banking Cyber Risks: A Synopsis of KPMG Collateral and Contacts" published from August 2013. Cybercrime is one of the fastest-growing yet hardest-to-control criminal activities. Many financial institutions see cybercrime as a serious danger to their survival. In order to perpetrate a range of crimes, more and more criminals are taking advantage of the speed, ease, and anonymity provided by contemporary technology. Because the internet is accessible across the globe, thieves may do almost any kind of wrongdoing from any location. That all governments must modify their physical controls to accommodate for cybercrime is underscored by this fact. While digital storage has the potential to help banks save costs and boost efficiency, it also raises the risk that private client information could be exposed. Financial institutions, IT firms, consultancies, and security firms have all been in the forefront of raising awareness of this problem. Several reports, both internal and external, have been published by KPMG on the topic. Our purpose in writing this report is to provide a synthesis of our research and to talk about the risks and the consequences such risks have for banks.

Cyber security risk management is a difficult endeavour. Since banks are under more close scrutiny from regulators and customers, their current

[5] https://www.statista.com/statistics/1012729/india-number-of-bank-fraud-cases/ accessed on 26 February 2023

[6] https://www.businesstoday.in/news-reel/video/dhfl-promoters-booked-for-indias-biggest-banking-scam-338870-2022-06-23 accessed on December 2023

[7] https://www.outlookindia.com/business/what-is-dhfl-scam-india-s-biggest-ever-bank-loan-fraud-all-you-need-to-know-about-rs-34-000-crore-dhfl-scam-news-204346 accessed on 25 February 2023

[8] https://www.deccanherald.com/business/business-news/a-look-at-some-of-the-biggest-bank-fraud-cases-that-hit- india-in-a-decade-1174934.html

[9] The King of Good Times, as Mallya was known as, is one of the biggest offenders when it comes to bank fraud. The businessman's now bankrupt. The Kingfisher Airlines owes more than Rs 10,000 crore to several banks, with SBI, PNB and IDBI all loaning hi...

[10] The Punjab National Bank scam was touted as India's biggest at Rs 11,400 crore and the main accused were jeweller Nirav Modi, Mehul Choksi, Nishant Modi, Ami Modi and others, including some PNB staff. The scam involved 'letters of undertaking' fraudu..

[11] Businessman Jatin Mehta’s Winsome Diamonds fraudulently acquired letters of undertaking from Indian banks and the fraud was caught for the first time in 2014. Mehta and his wife Sonia and their sons Vipul and SurajIt fled India and have left a loan d..

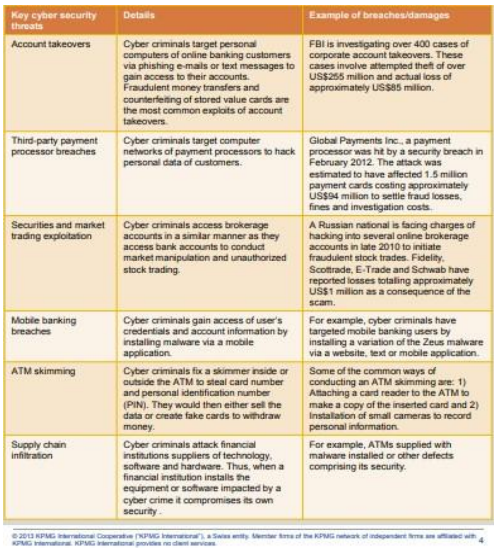
[12] Kanishk Gold Pvt Ltd was charged by CBI for allegedly cheating 14 banks led by SBI out of Rs 824 crore. The owners have been accused of taking huge loans for business and were detrimnetal to the banks' rights and interests,the lawsuit said, accordin..

[13] Gujarat-based pharma company Sterling Biotech Limited was involved in the Andhra bank fraud case as 4 directors of the company were named defaulters in the Rs 8,100-crore bank scam. Nitin Sandesara, Chetan Sandesara, Dipti Sandesara and Hiteshkumar N...

[14] Rotomac Global Private Limited of Kanpur, its promoter Vikram Kothari, and other directors were charged by the CBI of allegedly defrauding lenders for ₹ 750.54 crore. The company has a total outstanding of Rs 2,919 crore against a consortium of seve n...

[15] FIR was filed against former ICICI Bank CEO Chanda Kochhar, her husband Deepak Kochhar, and Videocon group MD Venugopal Dhoot for alleged irregularities in loans the bank to the group back in 2012. The case pertains to the time when Kochhar was the C...

strategy focuses on safety and compliance stakeholders. The need of safe and effective data management and storage is highlighted. The following are some of the most critical cyber security challenges affecting the banking industry, as identified by the Federal Bureau of Investigation (FBI):



Key cyber security threats	Details	Example of breaches/damages
Account takeovers	Cyber criminals target personal computers of online banking customers via phishing e-mails or text messages to gain access to their accounts. Fraudulent money transfers and counterfeiting of stored value cards are the most common exploits of account takeovers.	FBI is investigating over 400 cases of corporate account takeovers. These cases involve attempted theft of over US$255 million and actual loss of approximately US$85 million.
Third-party payment processor breaches	Cyber criminals target computer networks of payment processors to hack personal data of customers.	Global Payments Inc., a payment processor was hit by a security breach in February 2012. The attack was estimated to have affected 1.5 million payment cards costing approximately US$94 million to settle fraud losses, fines and investigation costs.
Securities and market trading exploitation	Cyber criminals access brokerage accounts in a similar manner as they access bank accounts to conduct market manipulation and unauthorized stock trading.	A Russian national is facing charges of hacking into several online brokerage accounts in late 2010 to initiate fraudulent stock trades. Fidelity, Scottrade, E-Trade and Schwab have reported losses totalling approximately US$1 million as a consequence of the scam.
Mobile banking breaches	Cyber criminals gain access of user's credentials and account information by installing malware via a mobile application.	For example, cyber criminals have targeted mobile banking users by installing a variation of the Zeus malware via a website, text or mobile application.
ATM skimming	Cyber criminals fix a skimmer inside or outside the ATM to steal card number and personal identification number (PIN). They would then either sell the data or create fake cards to withdraw money.	Some of the common ways of conducting an ATM skimming are: 1) Attaching a card reader to the ATM to make a copy of the inserted card and 2) Installation of small cameras to record personal information.
Supply chain infiltration	Cyber criminals attack financial institutions suppliers of technology, software and hardware. Thus, when a financial institution installs the equipment or software impacted by a cyber crime it compromises its own security .	For example, ATMs supplied with malware installed or other defects comprising its security.

(Sources:https://assets.kpmg.com/content/dam/kpmg/pdf/2013/09/isue-digest-Cyber-risks-for- banks-August-2013.pdf)

Precautionary Solutions[16]

Solutions that require users of computer systems and networks to undertake or abstain from acts that make them a soft target are called preventive measures. Simply put, these precautions make it more difficult for criminals to commit crimes in the first place. To name a few:

1. To avoid being a target of cyberstalking, one should avoid giving out any personal information.[xxxiii]

2. Never risk losing important files due of a virus by not regularly backing them up.

3. Avoid providing sensitive financial information such as credit card numbers, bank account details, etc. while using certain online financial portals if you have any questions about the legitimacy of the transaction.

4. You shouldn't use, save, or copy any files from an unknown source, whether they were obtained from the internet or received as an attachment in an email.[xxxiv]

Technological Solutions[17]

The IT sector is the original home of cybercrime. A cybercrime is any illegal conduct that makes use of computers. As a result, technological progress is the primary and, perhaps, most crucial tool in the fight against cybercrime.

CONCLUSION

To ensure the smooth execution of its cyber security agenda, the Indian government formed the Inter Departmental Information Security Task Force (ISTF), with the National Security Council serving as its coordinating body. When a cyber security crisis occurs in India, it is handled by the Computer Emergency Response Team of India (CERT-In). CERT-In does a variety of things to implement cyber security, including coordinating responses to security incidents and other major events, issuing advisories and time-bound advice regarding imminent threats, analysing product vulnerabilities, holding trainings on specialised topics of cyber security, and evolving security guidelines on major technology platforms.[18]

Corresponding Author

Renu Vijaywargia*

Research Scholar, Raj Rishi Bhartrihari Matsya University,Alwar-301001, Rajasthan

16 https://assets.kpmg.com/content/dam/kpmg/pdf/2013/09/isue-digest-Cyber-risks-for-banks-August-2013.pdf

17 India: An Overview of Cyber Laws vs. Cyber Crimes: In Indian Perspective by Rohit K. Guptaretrieved from http://www.mondaq.com/india/x/257328/Data+Protection+Privacy/An+Overview+Of+Cyber+Laws+vs+Cyber+Crimes+In+Indian+Perspective

18 Cyber Crimes: Law and Practices (.pdf); retrieved from http://www.img.kerala.gov.in/docs/downloads/cyber%20crimes.pdf