INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

www.ijlra.com
Volume 2 Issue 7 | March 2024
ISSN: 2582-6433

CYBERCRIMES AND ITS IMPACT ON BANKING INDUSTRIES

AUTHORED BY - JAAHNAVI MISHRA

ABSTRACT

in the era of the digital world where everything is shifting towards digitalization. the business sector has also geared up with their business activities using modern technology. Cyber technology provides a great height to organizations by raising their profit shares, especially to financial institutions by providing them the storage for data, online platforms for money transactions, and other online services where digital technology connects the world at a larger scale. As digitalization has gradually improved it has also created threats and challenges for financial institutions such as cybercrime. This research paper will analyze the impacts of cybercrimes in the banking industry which is spreading very speedily in the present time, cyber threats come up with many different challenges including from malware attacks to illegal access to customers' data. Beyond the legal aspect, the research will also look at how cybercrimes affect the reputation of organizations, and the preventive measures taken by banks to overcome the challenges.

Keywords- cybercrime, financial institution, digitalization

INTRODUCTION

Consider a global network enabled by digital technology, also referred to as cyberspace, that connects everyone on a single platform. The Internet is a vast platform that we use for many different purposes, such as shopping, social media, and financial transactions. In the digital era, banking institutions have also become key players. We may all prefer easier and more convenient banking services due to technological advancement. But as in the real world, a number of issues come up. The primary one is online fraud. These days, hackers and other criminals attack financial institutions heavily. It is very usual. The bulk of institutions have definitely relied on technology and digital networks for their operations, which raises the risk. of being a cybercrime victim.

ISSN: 2582-6433

This study attempts to examine the issue of cybercrimes in the banking sector by highlighting the relationship between data security and technology, enhancing the protection of our private information and financial transactions in online banking.

HISTORY OF CYBERCRIME

Cybercrimes initially began in the early days of technology and communication.in 1834 there were two thieves who used the telegraph system, gained access to financial markets, and stole data. Many experts consider this as the event of the first cybercrime and illegal activities rapidly started to begin in the field of technology. During the 20th century computing technology developed, and cybercrimes also evolved at the same time. A drastic change occurred in the history of malicious software intended to attack and disrupt computer systems in 1971 when BOB Thomas of BBN Technologies created it with the intent to harm the computer system. In the 1980s emails become a popular way of communication and by the 1990s, web browsers and computer viruses become popular. In these years hackers use email attachments to deliver malware and phishing scams and web browsers to spread computer viruses.[1]

It is important to understand the historical aspect of cyber-crimes which is diverse, complex, and developed by various significant events and developments. the examples given here are just a glimpse into the early instances of cybercrime events that led to the evolution and progression of these crimes.

TYPES OF CYBERCRIMES

There are many types of cybercrimes in India. here we discuss a few of the most common types of cybercrimes that we can see in our surroundings

- **Phishing** – it is a fraudulent activity to take the personal information of an individual which involves using false emails, websites, or messaging platforms in order to deceive people into disclosing their personal information such as passwords, usernames, and financial information.
- **Malware**- malware is a software program that is used to harm devices common example of malware is viruses that enter a device and start creating problems they may delete the

[1] Cybercrime: history, global impact & protective measures [2022], BLUEVOYANT, https://www.bluevoyant.com/knowledge-center/cybercrime-history-global-impact-protective-measures-2022 (last visited Jan. 26, 2024)

ISSN: 2582-6433

files or download some unwanted files, erase your disk drive, or corrupt your data. it also covers spyware, ransomware, trojans, etc.[2]

- **Identity theft**- it is a cybercrime in which the criminal uses the identity of the victim without permission to commit criminal acts and uses it for his benefit such as their name, social security number, and credit card information in order to make financial gains.
- **Hacking**- it is an illegal way of getting access to a system or computer with the intent to steal data, or documents and cause harm to it. they may use social engineering techniques or take advantage of the loopholes in software.
- **Cyberbullying**- it is an act of harassing, bullying, or threatening someone using online technology i.e. internet. cyberbullying includes coercion of a person to do something without his consent, spreading false information about that person, and sharing their private data. It is usually common among teenagers. According to a survey, 46% of the teens surveyed claimed to have suffered online harassment, while 24% of adults aged 26-35 have experienced cyberbullying.[3]

CYBERSPACE AND BANKING IN THE DIGITAL AGE

Cyberspace is a vast online area that offers a means of establishing global internet connections. It has a significant impact on how we live and how business is conducted these days. we can see it as one big virtual community where all of us are connected to each other through digital technology. Banking services are now quicker and more convenient for customers because of the banks' rapid advancements in this tremendous wave of digitalization. The digital age has made banking services more user-friendly, allowing people to save time and effort by performing additional online tasks including money transfers with a single click and online transactions using a phone. The use of banking and the Internet presents a number of risks and difficulties with this development, though. Threats from cybercrime have become a major issue as financial transactions move more towards the digital platform in order to commit any fraud or obtain unauthorized access to personal and sensitive data, hackers and cybercriminals are always coming up with new ways to take advantage of loopholes in online banking systems. In order to maintain the integrity of their systems and safeguarding the data of the customers requires the banking sectors and financial institutions to follow all the safety measures and make significant

[2] ibid
[3] *"Cyberbullying in India: A growing concern for parents and educators"*, Times of India Blog, https://timesofindia.indiatimes.com/blogs/voices/cyberbullying-in-india-a-growing-concern-for-parents-and-educators/ (last visited Jan. 26, 2024).

ISSN: 2582-6433

investments in cybersecurity services. Additionally, the customers are also required to be careful and aware of these preventive measures and must follow the measures like creating strong passwords, timely updating the software, and being careful of phishing scams.

CYBERCRIMES IN THE BANKING INDUSTRIES

Cybercrimes in the banking industry are becoming increasingly common and highly complex. they seriously hamper the security and reliability of banks. by using computer technology these criminals can identify the flaws and weaknesses in the banking system and use it for their own benefit which results in financial loss, damage to the reputation of financial institutions, and a decline in customers' trust towards the financial institutions. Let's examine some important and most common cybercrimes in the banking industry:

- **ATM skimming**

  A way to hack an ATM or POS is to place a skimming device that captures the data and reads the magnetic strips of debit and credit cards it is usually placed on top of the keypad, making it look like a real keypad. With the help of this device, skimmers can acquire the personal identification numbers of the customers and card numbers which are later used to carry out fraudulent transactions.

- **DNS Cache poisoning**

  It Is an act of putting false information in the DNS cache. DNS servers are used to speed up resolution response times by storing previously received query results in cache. By taking control of an affected system in DNS software, poisoning attacks against the server are executed. Consequently, the server inadvertently verifies DNS replies to make sure they originate from a reliable source. an attacker can hack the clients by spoofing an IP address; and DNS entries for a bank website on a given DNS server and replacing them with the IP address of a server they control.[4]

- **Ransomware attacks**

  It is a type of malicious software that looks at or encrypts customers' data, files, and devices. To obtain the decryption key the cybercriminals demand a ransom it has the potential; to affect the operational disruptions.

- **Credential stuffing**

  It is a type of cybercrime in which the criminal accesses the banking account without

[4]An Overview of Cyber Crimes in Banking Sector, Legal Service India - Law, Lawyers and Legal Resources, https://www.legalserviceindia.com/legal/article-7694-an-overview-of-cyber-crimes-in-banking-sector.html (last visited Jan. 30, 2024).

ISSN: 2582-6433

authorization by using a password and username that they have stolen from previous data breaches.

IMPACTS ON BAKING INDUSTRIES

Those who are attacked by cybercrimes may suffer long-term effects. the banking sector as well as the customers affected by it, affecting financial loss, reputation damage to the financial institution, and overall stability of the bank

i. Financial losses and operational disruption

Banks may suffer huge financial losses as a result of cybercrimes. Along with the significant financial loss. it also involves alterations to the regular operations of the institution, reputation damages, and legal liabilities toward the customers. The banking institution needs to calculate the financial loss as to how much money is lost which means calculating the money obtained through fraudulent activities, the cost that has been incurred to address the cyber threats, and the long-term financial impact on the bank.

Cybercriminals frequently carry out a complex transaction that causes harm to the financial institution and the customers. To understand this the bank has to keep an eye on how these criminals operate and how they find the weak spots by looking at this the banks can become more secure and can prevent these tricky and malicious activities.

ii. Reputation damage

The reputation of banks is hampered due to cybercrimes, trust of customers in the financial institution is weakened by reports of data breaches, ransomware attacks, or by illicit activities. Customers may withdraw money from their banks, potential customers may be afraid to connect with the banks and the bank's stock value may suffer if it is thought that susceptible to cyberattacks. It becomes difficult and time-consuming to restore the damaged reputation.

iii. Regulatory scrutiny

Regulations are scrutinized in response to cybercrimes as authorities look into the facts around the breach. The regulatory agencies look to evaluate whether the bank has followed the set guidelines and required compliances. In case of non-compliance, the bank needs to pay the penalties suffered by the increased regulatory burdens. When cybercrime takes place banks face

ISSN: 2582-6433

many challenges in meeting all these criteria which necessitates thorough evaluations of current policies.

iv. Legal consequences

The financial institutions that become the victim of cybercrimes may face legal consequences on several levels. Customers whose data has been stolen may sue for damages in addition the banks that do not follow sufficient safeguards for preventing cybercrimes may be legally held liable, and legal actions may have long-term effects on the financial institutions and put further financial burden on resources.

v. Increased cybersecurity costs

The financial institutions have to spend a lot of money to improve their cybersecurity after a cyberattack. In order to stop such incidents from happening, money is invested in the implementation of new security technology, and protocols, and conducting thorough audits Since the resources are being taken away from other strategic objectives, the institution's overall financial health is directly affected by the increased spending on cybersecurity.

vi. Global financial stability

Global financial stability is at risk from widespread cybercrimes that simultaneously target many banks. The potential for coordinated attacks to destabilize the financial markets, undermine public trust in the banking sector, and have a huge effect on the whole world. A security attack in one area can have far-reaching effects globally due to the interconnection of the financial industries with each other, Making cooperative measures to reduce systemic risks necessary.

In order to handle the complex issues raised due to cybercrimes cybersecurity measures must be continuously improved, collaboration within banking industries, and proactive risk management to be implemented.

CYBER ATTACKS IN INDIA -STATISTICAL DATA

A report by cybersecurity firm Cyfirma shows that between 2021 and September 2023, state-sponsored cyber-attacks on India increased by 278% during the period, and 14.3% of cyber assaults targeted enterprises that provide services, such as IT and BPO firms.

ISSN: 2582-6433

Targeted cyberattacks increased by 460% against government entities, but a significant 508% against startups and SMEs. India is the nation most frequently attacked in cyberattacks (13.7% of all cyberattacks), followed by the US, Indonesia, and China. Over the past three years, states have supported 68% of cyberattacks worldwide.

In India, this number was somewhat higher at 72%. There has been a noticeable change in threat players; only 6.4% of threats are coming from Pakistani actors, down from 79 % coming from China. In order to combat advanced cyber threats, the research highlights the necessity of better cybersecurity policy enforcement in India as well as raised awareness, particularly among SMEs and startups.[5]

INCIDENTS OF CYBER ATTACKS IN INDIA

- **Cosmos Bank malware attack in Pune**

One of the largest cyberattacks on an Indian bank at the time occurred at Pune, India's Cosmos Bank in 2018. Hackers got access to the bank's ATM switch server through malware, which allowed them to steal the personal information of several Rupay and Visa debit card holders. This led to almost 12,000 fraudulent transactions in 28 different countries, resulting in the siphoning off of about Rs 94 crore, or about $13.5 million. Additionally, the hacker started a swift transaction and transferred money to an account in Hong Kong. The bank suspended its online and mobile banking services, along with its ATM operations, as a result of the incident. Several people were found guilty and given sentences in relation to the cyber fraud case after the incident. The hack made use of duplicate debit cards.[6]

- **ATM system hacked**

A cyberattack targeted Canara Bank's ATM servers in 2018. Many bank accounts were emptied of 20 lakh rupees. Sources claim that over 300 consumers' ATM credentials were compromised by cybercriminals, making 50 victims in all. Slimming devices were used by hackers to obtain debit cardholder data. the value of transactions containing stolen data ranged from Rs. 10,000 to Rs 40,000. If ATM protection procedures are strengthened to prevent data misuse, it can be

[5]The Wire, https://thewire.in/tech/state-sponsored-cyber-attacks-against-india-went-up-by-278-between-2021-and-september-2023-report (last visited Jan. 30, 2024).
[6] Hindustan Times, https://www.hindustantimes.com/cities/pune-news/11-convicted-for-2018-94-crore-malware-attack-on-cosmos-cooperative-bank-101682270525442.html (last visited Jan. 30, 2024).

ISSN: 2582-6433

prevented.[7]

- **RBI phishing scam**

The Reserve Bank of India was not spared by the fraudsters in a bold phishing attempt of its kind. The phishing email, which appeared to be from the RBI, guaranteed the recipient reward money total of Rs 10 lakh rupees within 48 hours if they clicked on a link that led to a website that was an exact replica of the RBI's official website, down to the identical logo and web address. Subsequently, the individual is requested to disclose personal information, including his savings account number, PIN, and password. On the other hand, the RBI made a notice on its official website regarding the phishing email.[8]

CYBERSECURITY MEASURES IN THE BANKING INDUSTRY

1. **Comprehensive technological investment**

   Smart technologies used by banks to protect the information of the users including multi-factor authentication, strong walls, and secret codes(encryption), it is difficult for cyber criminals to steal it because of these security measures.

2. **Employee training programs**

   Training should be given to the employees and staff at the bank, to prevent the threat of cybercrimes. banks must ensure their employees are capable of handling and identifying the issues of cybercrimes. This will protect the customers against the malicious and fraudulent practices of threats.

3. **Security audits and expert collaborations**

   Banks are required to check and evaluate security measures frequently. banks also consult with experts and specialists who possess in-depth knowledge of cybersecurity. The financial institution must ensure that their customer's account is protected and that they are ready to handle any issues with will arise with time.

CYBER SECURITY CHALLENGES

- **Sophisticated cyber threats**

  as the advancement of technology takes place cybercrimes evolve with time and become

[7] An Overview of Cyber Crimes in Banking Sector, Legal Service India - Law, Lawyers and Legal Resources, https://www.legalserviceindia.com/legal/article-7694-an-overview-of-cyber-crimes-in-banking-sector.html (last visited Jan. 30, 2024).
[8] ibid

ISSN: 2582-6433

more complicated and multifaceted. this indicates that cybercriminals are defeating the security measures that are implemented by financial institutions through the use of sophisticated tools such as smart computers and software. Their goal is to take advantage of the loopholes in the security measures and obtain sensitive information without authorization.

- **Insider threats**

  Insider threats refer to the people who are employed in the institution such as partners or contractors who may accidently or purposefully do things that harm the company's security. Errors, ignorance, or in certain situations malicious intention could be the source of this. Keeping the surroundings secure requires managing these insider threats.

- **Supply chain vulnerabilities**

  Global supply chains, in which various institutions collaborate with each other to produce and transport goods and services, are how the institutions are linked together but there are vulnerabilities introduced by these links as well. The cybercriminals target the supply chains in an attempt to identify loopholes and obtain private information. They can affect multiple firms at once by a supply chain attack that has a wide range of implications.

- **The complexity of regulatory compliance**

  Organizations must abide by several cybersecurity laws and guidelines these guidelines provide how to handle, report, and protect the data. However, there are numerous regulations and each has different requirements, these are the source of complexity. Continuous efforts and resources are required from the organizations to adjust to the changes in these regulations.

THE FUTURE TRENDS

1. **Zero trust security model**

   The zero-trust security model is a paradigm that doesn't hold anyone inside the network parameter to be implicitly trusted. the users and devices internal and external are viewed. Under this framework as potentially unreliable. Internal threats and unauthorized access are less likely to occur because of this model's thorough inspection and authentication of access.in other words, the zero-trust model provides improved safety, enhanced compliance, and reduced risk of data breaches, which helps in the adaptation of changing needs and mitigation of cyber threats, also increases customers' trust, and makes it valuable for the banking sector.

ISSN: 2582-6433

2. **AI-driven cybersecurity**

   AI and machine learning tools are becoming essential tools of cybersecurity it works smartly and store data safely and they analyze large amounts of data to find trends and abnormalities linked with cybercrimes. By early threat detection and response automation, AI-driven cybersecurity solutions improve overall security by acting as a proactive defense. It offers various benefits including enhanced threat detection, improved accuracy and efficiency, adaptability and scalability, and compliance and regulatory support.

3. **Increased emphasis on cloud security**

   Cloud security, sometimes referred to as cloud computing security is a group of security controls intended to safeguard data, apps, and infrastructure that are hosted on the cloud. these safeguards provide data privacy protection, control over the data and resources access, and authentication of users and devices. They assist with regulatory data compliance as well. Cloud security is used in cloud environments to safeguard a business's data against hacker attacks, malware, distributed denial of services (DDoS) attacks, and unauthorized user access or use.[9]

CONCLUSION AND RECOMMENDATIONS

As technology advances rapidly, security threats are evolving too. However, there are still certain problems with the current system in India. There are gaps in the legal system and a lack of appropriate framework and specialized regulations to deal with cybercrimes. furthermore, there is a lack of tools and resources to deal effectively with cybercrimes. Still, a few recommendations might make the framework better.

Legislation pertaining to cybersecurity must be clear in order to address the growing threat of cybercrime. It must cover issues related to data protection, reporting of cybercrimes, and the consequences of doing so i.e. the punishment for cybercriminals. It is also essential to maintain these regulations by applying the most recent technological developments

Another crucial step is to promote collaboration between the private and public sectors so that they can jointly develop effective plans and strategies for the prevention of cybercrimes and

[9] What is Cloud Security? - Benefits of Cloud-Based Security | Box, Inc., Box, https://www.box.com/resources/what-is-cloud-security (last visited Jan. 30, 2024).

ISSN: 2582-6433

implement the finest cybersecurity safeguards in place. furthermore, it is important to ensure that law enforcement and cybersecurity personnel have the expertise to tackle cybercrimes. This can be easily achieved by providing funding for the training programs.

By addressing these issues and implementing important measures India can imprever-evolvingrity and it can create a more secure online environment to secure the nation from the ever evolving world of cyber threats.