LEGAL LOCK JOURNAL

2583-0384

VOLUME 3 || ISSUE 1

2023

CYBER CRIME IN BANKING INDUSTRY AND ITS IMPACT ON BANKING INDUSTRY

Sejal Dhakad[1]

Abstract

Computers are often used in cybercrimes as targets or as storage devices, depending on how the information they hold is altered or retrieved. Author will find that information which is changed or retrieved illegally and how the computer can be used to store information that will help with the crime's execution way. The Author will also learn about different kinds of cybercrime phishing, identity thefts, blackmailing and spoofing, worms and trojan horse and hacking, search engine, spyware, cyber terrorism etc. All sensitive organizations, including financial institutions, insurance, media, healthcare, security contractors, Governments, prominent businesses, financial institutions, and technology, are in significant danger from cyber-related crimes. Compared to other sectors, the banking industry carries more substantial risk. The Author will also try to shed some light on the many types of Cybercrime that affect the banking industry, the challenges the industry faces in preventing them, the impact of Cybercrime, and the measures taken by India and other nations to stop it from harming the banking industry.

Overview

Cybercrime is the deliberate, malicious use of information technology by cyberterrorists to harm and destroy the tangible and intangible property of others. The problem of Cybercrime transcends national borders and is global in scope. Blackmail, worms, trojan horses, malware, spoofing, data theft, search engines, and other cybercrimes are only a few of the many types of crimes performed against the banking industry. Cybercrimes can also range from terrorism to amateur hacking.

The banking sector faces significantly more significant risks. Information technology solutions have opened the door to a new world of business networking, e-banking, and the

[1] The author is a student of law at Indian Institute of Management, Rohtak.

Internet. These innovations are emerging to cut costs and provide quick, efficient, and time-saving transaction methods. The Internet has been a boon for the current pace of life. Still, it poses several risks to consumers and financial organizations, especially the banking sector. Many cybercrimes include Blackmail, worms and trojan horses, spoofing, identity theft, spyware, and internet sites. Numerous banks, financial institutions, investment houses, brokerage firms, and other businesses are the victims of cyberterrorism, which targets them and threatens to demand ransom payments to protect their confidential data and prevent severe losses.

1.1 What is Cybercrime?

Cybercrime is often described as Any unlawful conduct in which a computer, Criminal activity is either committed or made possible through the use of a communication device or computer network. It is possible for both individuals and groups to commit Cybercrime. Some cybercriminals are well-organized, use cutting-edge techniques, and possess advanced technical abilities.[2] Several hackers are beginners. When private information is intercepted or made public, whether legally or illegally, there are various privacy issues concerning Cybercrime.

Cybercrimes, such as espionage, financial theft, and other cross-border crimes, are committed internationally by both state-sponsored and non-state actors. Cyberwarfare is the term used to describe international border-crossing cybercrimes that involve at least one nation-state. Cybercrime, according to Warren Buffett, is the world's worst issue and poses genuine hazards to humankind.

According to a McAfee-sponsored analysis from 2014, Cybercrime costs the world economy $445 billion annually. The U.S. lost about $1.5 billion to online credit and debit card fraud in 2012.[3] In 2018, research Center for Strategic and International Studies (CSIS) research undertaken in collaboration According to McAfee, Cybercrime costs the global economy close to $600 billion annually. The 2020 Global Risk Report from the World Economic Forum states that organized cybercrime groups

[2] Mrs S. Kalpana & Dr. Mahalakshmi, *Cyber Crime: A Growing Threat to Indian E-Banking sector*, JETIR Volume 7, Issue 12, 1-6, (2020).

[3] Sumanjit Das & Tapaswini Nayak, *Impact of Cybercrime: Issues and Challenges*, IJESET, SSN: 22316604 Volume 6, 142-153, (2013).

are cooperating to commit crimes online, with a less than 1% chance of being discovered and prosecuted in the U.S.

Cybercriminals frequently do both at the same time. They may infect computers use them to disseminate malware along a system or to other computers initially. Some jurisdictions recognize a third type of Cybercrime in which a computer is used as an accomplice. One instance is using a computer to store stolen data. In comparison to 27, 248 cases in 2018, there were roughly 44, 546 cases reported under the subject of "Cyber Crime" in 2019. The result is, a 63.5% increase in Cyber Crimes was observed. The Information Technology Act, 2000, also known as the "I.T. Act," and the Rules enacted under it serve as India's legal foundation for cyber law.

1.2 Different Types of Cybercrime

1. Phishing - Phishing is a type of fraud in which private details such as Id Number, Visual effects, Payment Card details, Card expiry date, CVV number, and so on is stolen via email messages which appear to be from a respectable source.
2. Hacking - Criminal hacking is the process of getting unauthorized access to data on a computer or network. By taking advantage of vulnerabilities in these systems, hackers are able to acquire data ranging from private information and business secrets to government intelligence. Hackers also breach networks to interfere with government and business processes. Computer and network intrusions cost billions of dollars annually, claims the FBI.
3. Attack from Ransomware – A form of software known as ransomware prohibits people from accessing their computers and the data they have saved on. The computer could be locked, or the data stored on it could be stolen, deleted, or encrypted. Attackers using ransomware encrypt files and demand a ransom payment for the decryption key. Paying the ransom is frequently the simplest and least expensive way to regain access to files.

   To limit the attack surface and avoid ransomware attacks, organizations should To find and fix vulnerabilities, especially those on devices that are connected to the Internet, do routine vulnerability scanning.[4] They should also keep offline, encrypted backups of data and test backups on a regular basis. Patching and updating software and operating systems on a regular basis can also help to prevent ransomware attacks. Identity fraud -Occurs when someone takes your personal information and utilizes it without your knowledge or consent. Identity fraud instances include credit card theft, tax I.D. theft, and medical I.D. theft. When a thief obtains access to your credit card information and uses it to make unauthorized purchases, this is referred to as credit card theft. When someone steals your Social Security number, theyuse it to file false tax returns with the IRS or your state. When someone steals your Medicare ID or health insurance member number, this is known as medical I.D. theft.

4. Online harassment - Online harassment is the persistent or severe targeting of an individual or group through destructive actions on the Internet. It includes cyberbullying, cyberstalking, online impersonation, doxing, swatting, revenge porn, sextortion, and other forms of online abuse. Cyberstalking is the repeated and targeted intimidation, threats, and harassment of a single person. False accusations, defamation, and digital vandalism are all examples. Online sexual harassment refers to a variety of sexual misconduct on digital platforms. Those who identify as women and/or LGBTQIA+ suffer disproportionately.
5. Spamming: Spamming is the practise of sending unwanted commercial communications to a person by email, SMS, MMS, or another similar electronic messaging service. They may attempt to persuade the recipient to purchase a product or service, or tovisit a store's website to make a purchase, or they might try to con him/her into disclosing bank account or credit card information.
6. Virus, trojans and Worms - A computer virus is a programme that is designed to enter your computer, damage alter your files data, and replicate itself.

   Worms are malicious programmes that replicate themselves on the local drive, network shares, and so on. A virus is not a Trojan horse. It is a malicious

[4] Balaraj D B & Pradeepa Anand Shetty, *Cyber Literacy of Bank Customers – A Study in Udupi and D.K.* District, International Journal of social and Economic Research Volume – 9 Issue -3 ,1, 5-8, July-Sep (2019).

programme that masquerades as a legitimate application. Trojan horses, unlike viruses, do not replicate themselves, but they can be just as destructive. Trojans gain access to your computer through a backdoor, allowing malicious users programs to steal confidential and personal information.

7. Phishing - Phishing is a cyberattack that aims to divert traffic from one legitimate website to a phoney one.
8. Internet job fraud - Internet job fraud is a scheme to exploit people. of job seekers by promising them falsely improved jobs with higher pay.
9. Cyber Terrorism - An intentional attack by non-state actors, or the prospect of such an attack, with the intent to cause physical, psychological, political, economic, ecological, or other harm through the use of cyberspace is known as cyber terrorism. DDoS attacks, other kinds of malware, and social engineering are tools that cyber terrorists can use. Time and money are lost as a result of cyberterrorism.

1.3 Analysis of Cybercrime in Banking Sector [India]

Through the use of cutting-edge technology, the fourth industrial revolution has changed the way many sectors operate and is steadily working towards economic sustainability. Given the considerable growth in connections and productivity, this will likely present new chances for the banking sector to enhance their management, operations, and competitiveness. With great opportunities, it's also create a risk of Cybercrime and difficult to control. Cybercrime issues are even more serious in the banking sector, one of the most active economic sectors and closely tied to finance issues for all stakeholders in society. Cybercrime is a highly serious threat to any nation since criminals in the banking industry are frequently skilled, can access, manipulate, and target bank accounts, information systems, and more, and can operate internationally.

As we all know India is developing country and recently, we achieved economic growth, However, this also implies that the nation's reliance on technology increased, particularly in the financial industry making it more vulnerable to attacks from

Cybercrime.[5] While there have been few studies conducted domestically on such an important subject, little is known and what has been studied is sparse and incomplete. These studies also hardly ever address the most recent developments in the issue, and some may not be able to adequately depict the scope of Cybercrime occurring in India.

The banking industry went digital as a result of the COVID. Operations on the front end and the back end are now both digital.[6] With the advancement of technology, cyberattacks have been steadily rising, and attackers are aggressively searching for victims to launch malicious attacks on banking and financial institutions' sensitive data.

Indian banking industry has been the target of numerous cyberattacks. The use of internet banking and rapid digitalization have increased the number of cybercrime incidents. 248 successful data breaches by hackers and thieves were reported by Indian banks between June 2018 and March 2022.[7] In order to obtain consumer and employee information that they can use to steal bank data and money, cybercriminals attack the banking industry. Hacking, keylogging, viruses, malware, phishing, pharming, ATM skimming, and point- of-sale crimes are some of the main challenges the Indian banking industry faces. In 2018, hackers broke into Cosmos Bank and stole Rs. 94.42 crores. Almost 4.8 thousand instances of online banking fraud were reported in India in 2021 alone.

Cybersecurity threats are growing more prevalent in the Indian banking sector for a number of reasons, including the lax security of mobile and web services used for online banking. Because of the rise in cashless transactions and the use of digital currency brought on by the development of digital India, cybersecurity is crucial in the banking industry. Protecting data privacy requires taking all necessary security

[5] Vanya Gautam, India’s Banking & financial Services Sector Is Top Target for Cyber Attacks in Asia: Report, (Oct. 31, 2022, 13:40 PM).
[6] Ranjitha S, *4 biggest Cyber Security Threats for Indian Banking Sector*, Great Learning (Oct.27,2022), https://www.mygreatlearning.com/blog/biggest-cyber-security-threats-indian-banking-sector/.
[7] Shashank Shekhar, *Indian Banking Sector at forefront of cyber- attacks: What are major ways and way ahead*, Firstpost (Nov. 13, 2022, 18:41 PM), https://www.firstpost.com/opinion-news-expert-views-news-analysis-firstpost-viewpoint/indian-banking-sector-at-forefront-of-cyber-attacks-what-are-major-threats-and-way-ahead-11620701.html

precautions. Due to its growing reliance on internet banking systems, Cybercrime poses a serious threat to the Indian banking sector. To guarantee that banks have reliable cybersecurity protections in place, the government must take the appropriate actions. Due to the dependence of the banking industries, Cybersecurity worries are increasingly common with online banking because both mobile and web services often have a lax security mechanism.

ATM System hacked

In the middle of 2018, there was an attack on the Canara Bank ATM servers. Sources claim that hackers compromised the ATM login information of over 300 users, stealing 20 lakh rupees from multiple bank accounts.[8]

UIDAI Aadhaar Software hacked

One of the major data breaches that took place in 2018 involved the exposure of 1 billion Indian Aadhar card details. In its official disclosure of the data breach, UIDAI highlighted the breach of about 210 Indian Government websites. Aadhaar, PAN, bank account IFSC codes, and other user personal information obtained using hacked Aadhaar software were exposed in this data breach, and unidentified marketers were offering Aadhaar information for sale over WhatsApp for Rs. 500. Also, an Aadhaar card printing was available for just 300 Rupees.

SIM Swap Fraud - In August 2018, two Navi Mumbai hackers stole 4 crores of rupees through false SIM card information and unauthorized bank account transfers. They used online banking to conduct their transactions. The statistics and incidents surrounding the most recent cyberattacks in India serve as a wake-up call for all still-vulnerable financial sectors. Companies must take cybersecurity safeguards and adhere to the security best practices listed below.

Cyber Attack on union Bank of India - In July 2017, there was yet another catastrophic cyberattack that raised everyone's awareness The attack was directed at the Union

[8] Tanseem haide , *Expect accused of hacking ATM machine serves using modern gadgets arrested by delhi Police, Times of India*, (Dec. 2, 2021, 15:16 PM), https://www.indiatoday.in/india/story/expert-accused-of-hacking-atm-machine-servers-using-modern-gadgets-arrested-by-delhi-police-1883339-2021-12-02.

Bank of India, one of the biggest banks in India.[9] The attack began when a worker clicked on an email attachment. A malware attachment was included in the email. It gave the hackers access to the bank's computer system, allowing them to steal data from the bank. The email attachment contained a fake bank message. A virus attack that provided hackers access to Union Bank's data and enabled them to gain its access codes for the Society for Worldwide Interbank Financial Telecommunication was caused by an employee who trusted the email and disregarded the specifics (SWIFT). Via SWIFT, international transactions are carried out. The hacker sent $170 million to a Union Bank account at Citigroup Inc. in New York using these codes.

1.4 [International] Cybercrime in Banking Industry

The entire banking industry in the world is increasingly at risk from Cybercrime. The financial Sector now faces greater cybersecurity threats, in part because the cyber threat environment is deteriorating. In particular, state-sponsored assaults on financial institutions are increasing in frequency, sophistication, and devastation. Cyberattacks might undermine the security and confidence and risk financial stability, the G20 warned in 2017**.**

In a September 2021 study by the Conference of State Bank Supervisors (CSBS), more than 80% of bankers identified cybersecurity risk as the top internal risk as being "very important." In many nations, there is an increase in the regulation of financial institutions (F.I.s), with regulations for cybersecurity, data protection, and privacy that are continuously evolving.

The banking industry is negatively impacted by Cybercrime. A balanced scorecard-based study established that the banking industry is negatively impacted by the rising incidence of Cybercrime. Criminals were able to breach the security systems of central banks and move millions of dollars illegitimately across continents. According to one estimate, Cybercrime cost Asian businesses $81 billion in only one year, which is more

[9] Devidutta Tripathy, *India's City Union Bank CEO says Suffered cyber hack via SWIFT System*, REUTERS, (Feb. 18,2018, 2:43 PM), https://www.reuters.com/article/us-city-union-bank-swift/indias-city-union-bank-ceo-says-suffered-cyber-hack-via-swift-system-idINKCN1G20AF.

than a quarter of the $315 billion global cost.

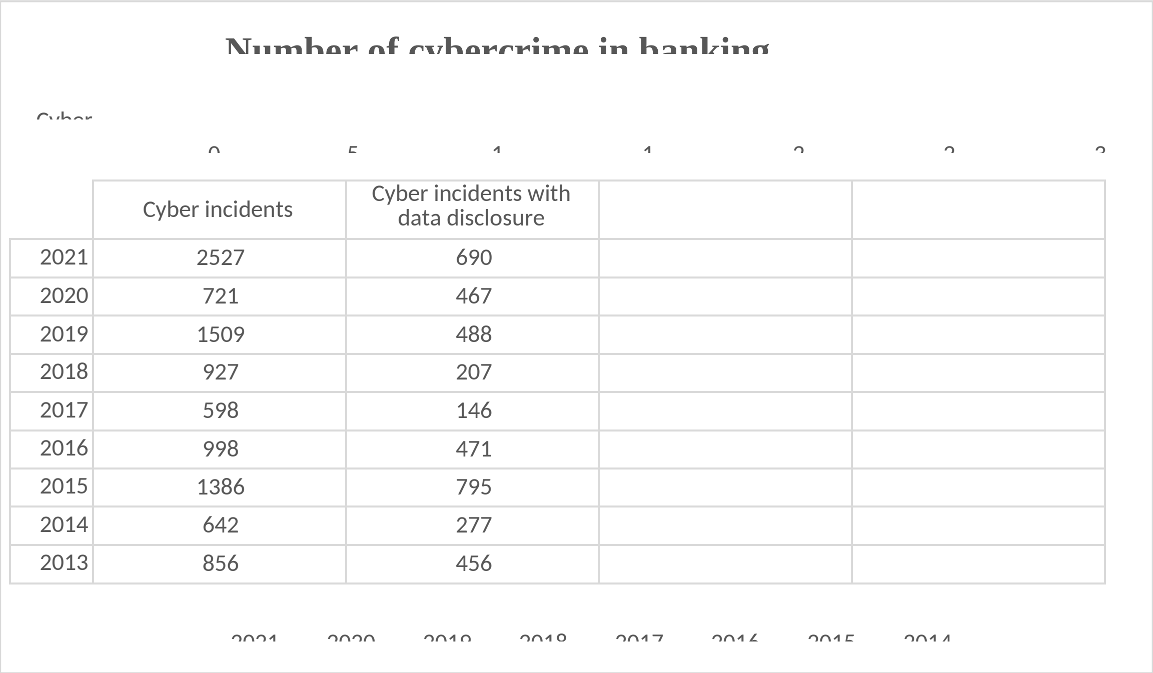
With the extensive use of the network by hackers to steal money from banks and the sheer volume of online attacks that its customers have had to deal with this year, SWIFT has been among the most vociferous in warning about the growing spectre of Cybercrime. In order to safeguard the reliability of the worldwide payments network, which handles over 25 million messages per day about the international payments of billions of dollars, SWIFT has also emphasized the necessity of banks to have a greater open to sharing information when they are hacked.

As a result, numerous parties are making significant efforts to attempt and solve this problem. It appears unclear that it will be sufficient to entirely eliminate the challenges that banks confront today on a global scale. Banking firms in less developed regions of the world are probably going to keep being highly vulnerable to Cybercrime, despite the fact that bankers in New York may be able to fortify their defences. Furthermore, given that these criminals have the benefit of being able to carry out attacks from anywhere in the world, it would seem that the logical countermeasures that must be developed will probably include a global coordinated effort among members of the banking industry.

Globally, there were 2,527 recorded cyber incidents in the banking sector in 2021, up from 721 the year before. The financial Sector now faces greater cybersecurity threats as a result of an increase in the frequency, sophistication, and destructiveness of state-sponsored cyberattacks against financial institutions. The G20 issued a cautionary statement that stated hacks may weaken the security and confidence and risk financial stability. More resources are being used by banks worldwide to resist cyber attempts.

The most significant risks to crime in the world today and in the future are financial and cybercrimes. Almost 60% of police respondents worldwide consider crimes including money laundering, ransomware, phishing, and online frauds to be extremely high or high threats.

1.5 Amount of cyberattacks on the banking industry globally between 2013 and 2021



	Cyber incidents	Cyber incidents with data disclosure		
2021	2527	690		
2020	721	467		
2019	1509	488		
2018	927	207		
2017	598	146		
2016	998	471		
2015	1386	795		
2014	642	277		
2013	856	456		

Cyberattacks in banking Industry at International The 2014 JP Morgan data breach

Tens of millions of people, seven million organizations, and 83 million consumers were impacted by the Data Breach. Five people stole email, address, contact information, sparsely distributed, and other customer information from JP Morgan and other associated banking institutions at the same time using spyware, social control, and spear-phishing attacks. The JP Morgan hack is noteworthy for a few more reasons in addition to the extent of the leak. First off, JP Morgan was spending $250 a year on information security at the time of the incident. However, all of that money was for nothing because one server was still operating without two-factor authentication. Second, of all the incidents mentioned, this is the only data breach in which the offenders have been apprehended.

Bank of America

Around $1 billion has been spent annually by Bank of America on cybersecurity. According to The bank's chief operations and technology officer, Cathy Bessant, spending on cyber security has increased recently. One of the banks targeted by denial-of-service attacks in 2012–2013 that clogged their servers with unwanted traffic and prevented customers from using online banking was Bank of America. A timeline shows that financial institutions have been the subject of numerous cyber incidents since 2007.

JP Morgan Chase

The most recent cyberattack on JPMorgan Chase occurred in 2022[10], when a Russian hacktivist organization by the name of Kill net claimed to have blocked J.P. Morgan's infrastructure. Nevertheless, the bank maintained that the attack had little effect on its business. 76 million homes and seven million small companies had their accounts compromised as a result of the 2014 JPMorgan Bank data hack.

In these attacks, phoney traffic was sent to the websites of those banks by thousands of stolen applications servers. Using specialized software known as Carberp, a cybercrime group by the name of Carbanak was able to steal from over 100 banks worldwide. A targeted spear-phishing campaign that was directed at bank tellers and administrators was used to disseminate Carberp. Once installed, it would download a typical remote-access programme that enabled the attackers to navigate the network until they located what they were seeking for: access to the SWIFT payment system.

One of the biggest challenges to financial services is phishing. In Q1 2021, the finance industry was the one that phishing assaults were most focused on. According to the Anti- Phishing Working Group (APWG), financial institutions were the target of phishing attempts the most frequently in Q1 of 2021. The financial services industry was the target of nearly 50% of detected phishing attacks, according to Akamai's 2019 State of the Internet report.

[10] SentinelOne, The Most Devasting Cyber Attacks on Bank in recent history, SentinelOne blog (Aug. 10,2016,12:34 PM), https://www.sentinelone.com/blog/the-most-devastating-cyber-attacks-on-banks/.

2.1 Impact of Cybercrime in banking industry and difficulties and challenges

Cybercriminals are increasingly focusing on the banking business, and it can have a big influence on this industry. One of the most frequent types of attacks is phishing issues with cybersecurity in the banking industry. The frequency of cybercrimes has escalated it has improved over the years to the point that it is now believed that they are one of the biggest threats to the financial Sector. Hackers' technology and skill have advanced, making it challenging for any banking sector to withstand an attack. Banks may suffer considerable financial losses as a result of cyberattacks due to fraudulent transactions.

It is not unlikely that a significant hack might cause a bank to fail. Virtually all financial institutions have been the victim of a cyberattack of some kind, and the frequency of attacks is rising. According to the Boston Consulting Group, financial institutions are 300 times more likely to encounter them than other institutions. Recovery from a breach can be very expensive and time-consuming. Cybercrimes can cost banks more to recover from than any other sort of business, and bank breaches have surged by more than 400% since 2018.

As a result of the increase in mobile devices with internet connectivity, cybercrime cases have rapidly increased. Nowadays, smartphones are used for a variety of online activities like online banking, shopping, and paying utility bills, making them a prime target for thieves looking to obtain sensitive data. The primary driver of Cybercrime over the past several years has been financial gain, which has consistently outpaced other incentives like retaliation, extortion, and political purposes. Alarmingly, due to a lack of knowledge about the standard precautions to prevent against cunning cybercriminals, simple phishing attempts have a success rate of 45%.

In 2020, there will be recorded around 290,000 cyber security incidents involving banking.[11] Minister of State for Electronics and IT Sanjay Dhotre, stated in a written

[11] The Economic Times, Over 26,100 Indians Website hacked in 2020 as Per CERT -In data : Sanjay Dohtre.

reply to the Rajya Sabha that according to data reported to and monitored by Indian Computer Emergency Response Team (CERT-In), a total of 1,59,761; 2,46,514; and 2,90,445 cyber security incidents pertaining to digital banking were reported during 2018, 2019, and 2020, respectively. Phishing assaults, network scanning and probing, malware, and website hacking were some of these occurrences. The Minister pointed out that the growing use of e-commerce and non-banking financial businesses (NBFCs) has also broadened the application of digital payments. According to him, the percentage increase in digital transactions from 2018 to 2020 will be 46%. From 3,134 crore in the fiscal year (F.Y.) 2018-19 to 4,572 crore in the following year, more transactions were made digitally. In response to a different inquiry, the minister stated that 9,849 websites, web pages, and accounts would be blocked in 2020. In 2018 it was 2,799, and in 2019 it was 3,635.

According to him, Section 69A of the Information Technology Act gives the government the authority to block any information produced, transmitted, received, stored, or hosted in any computer resource in the interest of India's sovereignty and integrity, defence, security, good relations with other countries, or public order. In response to a different query, Dhotre stated that, according to National Crime Records Bureau (NCRB) data, 6,233 incidents of fraud and cheating (using communication devices as a medium or target as per the Information Technology Act 2000) were filed in 2019. According to NCRB, there were 3,466, 3,353, and 6,233 cases of fraud and cheating (using communication devices as the medium or target in accordance with I.T. Act 2000) for cybercrimes in the years 2017, 2018, and 2019, respectively.

2.2 Difficulties and Challenges

1. **Technology factor -** Cybercrime has evolved along with technology, but security experts and law enforcement authorities have not yet caught up with the offenders. Businesses and people use technology more and more as it develops and matures, which also increases the attack surfaces on those technologies. Because to issues including user ignorance, an availability of data, and simple access to the Internet, cybercrime problems are predicted to

persist over the next decade. A few important variables that have contributed to the continued cybercrime activities are briefly discussed by the Author. The elements influencing the development of cybercrime technology, as well as its accessibility, underground market, and numerous participating jurisdictions. The essay offers the availability of technological resources, business data, the speed of the Internet, training, and lack of legal framework by countries to prosecute cybercriminals are all contributing to the growth of the cybercrime sector. The speed of the Internet, hacking, and the accessibility of anti-forensics and computer hacking tools are further factors that have contributed to the high rate of Cybercrime. Management's lack of commitment to advanced security investments also fosters a climate where computer thieves can exploit network and system flaws and engage in a variety of cybercrimes. One of the biggest problems that everyone is currently dealing with is cybercrime remedies to the issues raised**.**

2. **Availability of data -** Data creation and storage have become much easier because of technology like mobile phones and high-speed Internet. Everyone can now collect and keep data thanks to these technologies, including businesses, organizations, and people. Due to technology, companies are now able tostore a lot of data. Therefore, personal data and customer information maintained by corporations will continue to be a target commodity in the cyber underground market. The thieves either utilize malware or direct database access to take information. Businesses transfer their data to their third-party contractors to save the expense of managing and retaining it. Because the company lacked third-party control to make sure the third-party provider was storing and keeping the data securely, this business decision resulted in data leakage

   Employees must be taught suitable data handling techniques in order to reduce the dangers of data theft. Management must make an investment in the purchase of security solutions, including intrusion detection systems, antimalware software, and anti-virus software. Risk analysis, testing, and auditing must be frequently performed by security professionals to determine whether apps where data is stored are secure. Security professionals must promptly share the outcomes of their testing with information technology decision-makers. One of the best ways to prevent attacks on systems that store sensitive corporate data is through regular vulnerability scanning and timely patching.

3. **Cybercrime underground market -** The underground market for Cybercrimehas been boosted by pharming and phishing activities. Illegal goods and services are traded in the cybercrime market. Social engineering methods can be used by criminals to deceive their victims into giving up personal information for this kind of trading. Most people do not believe that every employee of an organization needs to participate in basic awareness training, despite the fact that some private corporations and government organizations have made it necessary. The majority of managers think that I.T. staffers who maintain company systems should attend awareness training. Resources must be pooled by groups of people and organizations in order to stop criminal activity in an underground market.

   The psychology and conduct of contemporary cybercriminals must be studied, and organizations and individuals must support this research. Practitioners of cyber intelligence must actively create the tools and procedures necessary to disrupt the operations of the digital black market.

4. **Multiple jurisdiction** - Many continents are connected by the internet and computer networks. Criminals are now able to launch an attack from anywhere online. In recent years, Cybercrime affecting various jurisdictions has increased. An act of Cybercrime in one region can spread across numerous jurisdictions with the use of the Internet.

   The nation, states, and regions can work together to address the difficulties that many jurisdictions pose. Countries, including Ghana, are currently working to resolve this jurisdictional issue, but progress has been extremely slow. Programs to combat Cybercrime must be centrally coordinated by leaders of nations, states, and regions. To assist stakeholders in streamlining their efforts, the programmes must be held at both the regional and international levels.

Global Cyber Laws must be implemented by international communities. To curb such actions, there is a rising necessity for the creation of global Cyber Cops and cyberspace taskforces. To coordinate and manage common and easy computer-related offences, an international criminal court must be established. To ensure proper prosecution of crimes committed in cyberspace, The International Cyber Crime Court system must be established. Last but not least, the international criminal justice system must strive for internal cybercrime law systems to be in perfect accord.

2.3 Protective methods to control Cybercrime

We people might believe that hackers obtaining your financial information is the only type of Cybercrime about which we need to be concerned.[15] It might not be that easy, though. Beyond simply the most fundamental financial worries, there are many more. More threats emerge every year as Cybercrime continues to develop.

As you discover and read about the various types of cybercrimes that occur, you might be inclined to give up using the Internet altogether. That's not possible in the 21st century.

Instead, it's a good idea to comprehend Cybercrime because that could be the first step in helping to secure your data and/or yourself. Other crucial actions include knowing who to contact when you observe others engaging in criminal activity online and taking some simple precautions.

Everyone who uses the Internet should practise some basic safety precautions. You may protect yourself from the different internet crimes that are currently being committed by following these tips.

1. Use an entire **Internet security suite** - Consider using reputable security software, such as **Norton 360 with LifeLock Select**[12], It helps to safeguard your personal and financial data online and provides complete protection for

[12] Caroline Duncan, *How to protect your organization Ransomware attacks Exploiting The COVID-19 situations,*(Apr. 10, 2020 8:29:49 PM).

your devices, online privacy, and identity.

2. Use **Strong Password** - Avoid using the same **passwords** across many websites, and change it frequently. Make them challenging. That entails utilizing a minimum of 10 different letters, numbers, and symbols. You can keep your credentials secure by using a password management tool.
3. Keep your **software updated** - This is incredibly important for your operating systems and internet security software. In order to access your system, cybercriminals usually leverage known exploits, or flaws, in your software. By fixing those bugs and exploits, you can reduce your risk of being a victim of Cybercrime.
4. Understand what to do if you end up a victim - You must notify the local police and, in some situations, If you believe that you are a victim of a cybercrime, contact the Federal Trade Commission. Even though the offence looks little, it is nonetheless important. Your information might help law enforcement in their investigations or stop criminals from taking advantage of other people in the future. If you think cyber thieves have stolen your identity. Here are some of the recommendations for you consider doing.
    - Get in touch with the companies and banks where you are aware of fraud.
    - Get your credit reports and place fraud alerts.
    - Inform the FTC about identity theft.

.

5. Manage **Social media settings** - Keep your private and sensitive information secure. The less information you give publicly, the better **because social engineering** cybercriminals may frequently obtain you can tell a lot about you from a small number of data points. For instance, you might divulge the answers to two frequent security questions if you post the name of your pet or disclose your mother's maiden name. Avoid clicking links in **spam emails** or on suspicious websites - By clicking on links in spam emails, other unsolicited messages, or unknown websites, consumers can also become victims of Cybercrime. To maintain your online safety, avoid doing this.
6. Check your **bank statements** - It's crucial to recognize when you've become a

victim of Cybercrime right away. Keep a watch on your bank statements and check with the bank about any strange activities. The bank has the authority to look into potential fraud. A competent antivirus programme will defend you against the risk of online crime.

7. Take precautions to help safeguard yourself from **identity theft** - When someone illegally gets your personal information through fraud or deception, usually with the intention of making money, it is called identity theft. How? For instance, a burglar may deceive you into providing personal information online or may steal your mail to gain access to account information. Protecting your personal information is crucial in light of this. In particular when using public Wi-Fi to access the Internet, a VPN, or virtual private network, can assist in securing the information you send and receive online.

Cybersecurity Threats to banking industry

Threats are constantly evolving, and the cybersecurity landscape is constantly changing. Since there are enormous financial sums at risk and the potential for considerable economic upheaval if banks and other financial systems are hacked, the stakes are high in the banking and financial industry. Raising staff knowledge of cybersecurity issues and utilizing cutting-edge communication technologies like Desk Alerts to cut through the digital noise and ensure that crucial information is being received should be a top focus for banks.

3.1The significance of understanding cybersecurity trends

In contrast to other businesses, ransomware assaults in the banking sector climbed by a staggering 1318% in just the first half of 2021, according to a Trend Micro analysis. Financial institutions undergo cyberattacks 300 times more frequently than other industries, according to a survey cited by the New York Federal Reserve, demonstrating how appealing this industry is to cybercriminals.

The following are the primary causes to be cautious about cybersecurity trends:

- More financial transactions than ever before are digital, thanks to a surge in cashless transactions.

- Customers' data may be compromised by the banking industry's poor cybersecurity.
- Recovery from a breach can be very expensive and time-consuming.

3.2The major cybersecurity threats to banks in 2022:

These are the main dangers that banks and other financial institutions are expected to face throughout 2022.

1. Ransomware - For several years now, Ransomware has been a huge nuisance for businesses all over the world, and it doesn't appear that this will change anytime soon. This type of Cybercrime locks users out of the system and encrypts user files before asking money to let users back in. Companies hit by ransomware attacks may experience prolonged system crippling, especially if they don't have backups. Moreover, paying the ransom demanded by these hackers does not guarantee that access to your systems will be re-established.
2. Ongoing dangers of working remotely - The use of remote work, hybrid workforces, and cloud-based software platforms has almost become standard as the pandemic approaches its third year. Additionally, this implies that financial organizations now more than ever have possible cybersecurity weaknesses. More caution is required because employees are no longer always accessing data on the organization-controlled systems and networks.
3. An increase in cloud-based cyberattacks - Cybercriminals have pounced on the fact that more software systems and data are being housed in the cloud, making cloud- based attacks one of the most pervasive cyber threats to the banking sector. In order to prevent damaging breaches, banks must make sure that the cloud infrastructure is configured securely.
4. Social engineering - One of the most common biggest dangers to banking and finance. Humans are frequently the weakest link in the security chain since they can be duped into divulging important information and login credentials. Customers and employees of a bank may both be impacted by this. Social engineering can take many different forms, such as phishing, whaling, or the

distribution of fake invoices that appear to be from a reliable source. It's crucial to keep your staff up to date on social engineering techniques and how these dangers are developing.

5. Supply chain attack - Targeting a software company and then distributing malicious code to customers and other parties in the supply chain via products or updates that superficially appear to be legal is becoming an increasingly common practice among hackers. By these attacks, fraudsters are able to access the networks of the supplier's clients and corrupt the distribution systems.

3.3 Cybersecurity challenges banks faced

It can be difficult to try to put cybersecurity mitigation methods into practice in the banking industry. The following are a few of the major obstacles that banks must overcome:

1. A cybersecurity skill gap occurs when the demand outweighs the supply of qualified workers.
2. Uninformed staff members whose cybersecurity awareness training is either insufficient or out of date and does not take new dangers into account.
3. inadequate funding to address cybersecurity concerns.
4. Employees' usage of shoddy credentials facilitates hackers.
5. Those looking to take advantage of mobile devices and banking apps target them.

4.1 Steps taken by India and other countries to control Cybercrime in the banking industry

India

In terms of generating cash and ensuring that key services run smoothly, banks are crucial. Despite setbacks like the current pandemic, they must continue to serve customers and country profitably while offering comprehensive and effective services.

For banks to operate effectively, boost efficiency, stay competitive, and grow, digitization is probably essential. In order to survive and grow after the pandemic, banks will need to step up their adoption of technology (such as digital banking, remote access, and cloud) and enable continual digital transformation.

Also, this implies that banks will probably continue to endure a variety of cyberattacks. Banks' use of information technology has expanded quickly and is now a key component of their operational strategy. In the recent past, cyber incidents and attacks have multiplied in quantity, regularity, and impact, particularly with regard to the financial Sector, especially Urban Co-operative Banks (UCBs) So that they can stop, identify, respond to, and recover from cyberattacks, UCBs must now strengthen their security posture. In light of this a, circular DCBS.CO.PCB.Cir.No.1/18.01.000/2018-19 dated October 19, 2018 A directive defining fundamental cyber security measures was sent to each UCB.

.

The Indian government has taken a number of actions to stop and lessen cybercrime-related events. To address issues relating to Cybercrime in a thorough and coordinated manner, it formed The Indian Cyber Crime Coordination Centre. This platform for investigating all aspects of cybercrimes, creating reports on cybercrime threat intelligence, and coordinating recurring discussions on cybersecurity issues among law enforcement, academia, researchers, and other interested parties.

To stop cyberattacks, the financial industry must implement cybersecurity measures and follow security protocols. Financial institutions must have the tools they need to handle cybercrime incidents. Because of the rise in cashless transactions and the use of digital currency brought on by India's digital transformation, cybersecurity is crucial in the banking industry. Protecting data and privacy requires taking all necessary security precautions.

The Global Programme on Cybercrime was developed by the United Nations Office on Drugs and Crime (UNODC) to provide member nations with capacity-building and technical support in their fight against cyber-related crimes. Information on national laws, best practices, technical aid, and international cooperation is available from the

Global Programme on Cybercrime. It adapts to the needs that are seen in developing nations by helping its members avoid and combat Cybercrime in a comprehensive way.

Specific laws to prevent cybercrimes are provided by the Information Technology Act 2000 (I.T. Act)[13] and the Indian Penal Code 1860 (IPC)[14], however fraudsters' misdeeds involving net banking are still rising quickly. The Reserve Bank of India (RBI) has released a thorough Cyber Security Framework for all scheduled commercial banks in order to solve this issue. This framework mandates that banks follow stringent data security and cybersecurity procedures. Banks that failed to follow the framework or reported cyber events were penalized by the RBI. The I.T. Act's purview should also be widened to provide the legal foundation for cyber regulation in India. Moreover, awareness efforts should be launched to inform people and businesses about cyber threats and how to defend oneself against them. Third, banks should implement internal dispute resolution mechanisms that can spot internal internet banking frauds.

.

Also Government ISTF, an Inter-Departmental Data Security Team, has been established to guarantee data security. In order to stop Cybercrime, the government also raises awareness about it and issues alerts and recommendations. The Information Technology Act of 2000 and the National Cyber Security Policy of 2013 are two examples of the different cybersecurity laws and governing bodies in India. It is crucial that both banks and customers take the necessary precautions to safeguard themselves from Cybercrime. Setting secure passwords, keeping social networking sites in private mode, and putting cybersecurity rules and regulations into effect are a few of these precautions.

Through the Cyber Crime Prevention Against Women & Children (CCPWC) scheme, the Ministry of Home Affairs (MHA) has made financial aid available to all states and union territories in order to support the mechanism for combating cybercrimes in a thorough and coordinated manner. In cases of non-compliance with their cybersecurity

[13] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

[14] Indian Penal Code 1860, No. 45, 1860 (India).

standards, banks and the financial Sector are subject to fines under the Reserve Bank of India (RBI) Act of 2018. Banks must develop and submit their cyber crisis management strategies, put into practise corporate-approved information security policies that specify cybersecurity readiness, and enforce DMARC security measures, according to the RBI. These rules must be adhered to by all Indian banks in order to standardize cybersecurity standards for payment processing and tackle business challenges in a digital environment.

People can use antivirus software, create strong passwords, keep social networking sites secret, report any suspicious behaviour online or offline, avoid clicking on strange links or downloading attachments from unknown sources, all of which can help to prevent Cybercrime in India. Companies must put in place cybersecurity safeguards such as firewalls, intrusion detection systems, encryption technology, access control mechanisms, routine data backups, and employee awareness training programmes.

4.2 International

The worldwide banking industry is increasingly at risk from Cybercrime. The Global Programme on Cybercrime, financed by Australia, Canada, Japan, Norway, the United Kingdom, and the United States, is made to adapt to the needs that have been found in developing nations by assisting Member States in preventing and combating Cybercrime holistically. Information on national laws, best practices, technical aid, and international collaboration are all provided through the programme. The UAE has been at the forefront of the region's efforts to reduce the frequency of cyberattacks by adopting decisive and aggressive measures. Adoption of more thorough and simplified laws and regulations with harsher punishments is key to the region's strategy and success in combating cybercrimes.

One of the industry's most susceptible to cyberattacks is the financial one. Strong corporate policies that ensure proper protection of customer data, ensuring employee safety regulations, and implementing proper checks including user account verification, user login monitoring, and password security to bring accountability are just a few of the key measures that can be taken to prevent such crimes. consisting of a collection of industry standards and best practices that assist firms in voluntarily managing cyber-risk. The regulatory authorities might use this framework as a strategy to improve the cybersecurity of banks.

Countries are taking a variety of actions, including enacting thorough laws and regulations with harsher penalties, putting robust corporate data protection policies into place, assuring staff safety standards with proper checks, including user account verification, and more. To further improve banks' cybersecurity, regulatory authorities are employing frameworks made up of best practices and industry standards that assist firms in voluntarily managing cyber-risk.

Suggestions

By having strict corporate policies that assure effective client data protection, the banking industry can combat Cybercrime. To maintain employee accountability, it is important to implement suitable checks, such as user account verification, user login monitoring, and password security. Banks should use cutting-edge methods that identify Cybercrime based on patterns seen in website navigation or transactional activity. Smart cards, a pin, facial recognition technology, and fingerprint sensors are a few examples. Fighting cyber threats at all levels is essential, as is informing customers of any shady activity occurring in connection with their bank accounts. Every bank must send out notifications and automatic communications to customers confirming the authenticity of a transaction. Building up a bank’s cybersecurity is not a one-time exercise but a constant process. Systems need to be regularly checked by surveillance technologies to identify any flaw that has been generated. Banks must regularly update their risk management plans.

With its headquarters in Abu Dhabi, the new networking and cybersecurity operation centre was formed by the Central Bank of the UAE with the goal of strengthening the UAE's financial Sector's I.T. defences against cyberattacks. Companies may advise installing new firewalls, anti-keylogging encryption software, endpoint security, multi-factor authentication, password and SSH key management, and other security steps to strengthen system security and reduce threats. Employees should receive cybersecurity awareness training so they can recognize malicious links or phishing scams. Banks can get a voluminous array of cybersecurity resources from the U.S. government.

Conclusion

The Internet is a global phenomenon. Thus, it is likely to draw many types of criminal activity. India has taken a big stride towards eliminating Cybercrime with the passing of the Information Technology Act, RBI policies and the Indian Cyber Crime Coordination Centre, Government policies giving of exclusive powers to the police and other authorities to combat Cybercrime. The power of the human intellect is beyond comprehension. Cybercrime cannot be eliminated from the Internet. You could look them over. History has proven that no policy has ever been able to eradicate crime globally. The only way to stop crime is to educate people about their rights and obligations such as making reporting crimes a shared social responsibility and to enforce the law more strictly. People must be knowledgeable about their qualifications and Banks must take extra precautions to prevent misuse and must work hard to raise client awareness and protect them from con artists. These steps can improve banking industry cybersecurity.