UNIQUE LAW

JOURNAL OF UNIQUE LAWS AND STUDENTS

EST. 2020

JOURNAL OF UNIQUE LAWS & STUDENTS

LLPIN: **AAS-8750**
WEBSITE: UNIQUELAW.IN
EMAIL: PUBLISH.JULS@GMAIL.COM

ABOUT US

"Journal of Unique Laws and Students" (JULS) which shall provide law students, young lawyers and legal professionals to deliberate and express their critical thinking on impressionistic realms of Law. The JULS aims to provide cost free, open access academic deliberations among law students and young lawyers. The ISSUE III of Volume 1 focuses on three themes i.e. (i) Arbitration Law (ii) Competition Law, and (iii) Criminal Law.

The journal strives to contribute to the community with quality papers on a vast number of legal issues and topics written by authors from various groups that have been reassessed and revised by our editorial team to reach the highest possible standard.

UNIQUE LAW is a law related Ed-tech premier start up in India that excels in imparting legal education. It is a registered entity under the name Ansh LexPraxis Legal Education LLP. The said LLP is recognized as a start-up India Initiative by Government of India's Ministry of Commerce and Industry and DIPP63504.

DISCLAIMER

This third issue of the Journal of Unique Laws and Students can be downloaded from:
https://www.uniquelaw.in/volume-i-issue-iii

PREFACE

On looking today scenario, there are numerous issues to know about. Our journal`s Issue III of Volume 1 has work on three crucial themes namely Criminal law, Arbitrational Law and Competition law. We have tried to cover these wide topics with the relevant research and landmark judgments. We have used standard of words for the explanation, evenly attempted to clear the concepts and presented captivating writing to the readers. The works also contains some suggestions in respective fields.

The views expressed in the articles are purely and solely of the authors and the entire team of the Journal has no association with the same. Although all attempts have been made to ensure the correctness of the information published in the articles, the Editorial team shall not be held responsible for any errors that might have been caused due to oversight or otherwise. It is up to the rest of us to help make the journal a success story in the next several years.

ADVISORY BOARD

EDITORIAL BOARD

EDITOR'S NOTE

Unique Law was established in the month of April 2020 and cheerfully brings **Volume 1 Issue III** of **Journal of Unique Laws and Students (JULS)**. This journal has become a successful climb in reaching to our goal of gaining visibility in the academic front and becoming a great platform in education community.

The journal aims to present merit papers on the numerous legal issues and these topics are authored by various groups of individuals that have been reappraise and emended by our team of editors to attend the highest possible excellence.

We thanks to all our authors for their obedient submission to the third issue of the Journal by Unique Law and also for their productive cooperation with the editorial team to garnish their work with perfection. We would also like to express our gratitude to our diligent editorial board, whose restless support and commitment made this Journal's Issue III a success.

TABLE OF CONTENTS

CYBERCRIME: A MULTIFACETED ONE

Author: Mitali Aryan*

ABSTRACT

Cybercrime has caused widespread damage to personalities, companies, including the city council. Computers have unleashed an era of greater efficiency and creativity. Communication and connectivity have reached new heights in the last twenty years. The Internet started a new revolution, the online revolution. As the masses are accustomed and inclined to their daily activities online, most are looking for easy money and information. This criterion represents modern criminals who, in addition to the availability of extensive equipment to access almost all systems, enjoy the anonymity of boundless cyberspace and therefore take human error and system vulnerabilities for granted. The batch consists of these cyber criminals, malicious hackers, malicious hackers, and spammers. This paper attempts to understand cybercrime on a long continuum, starting with the doctrinal research method part. Research and analysis of the world's leading cybersecurity companies were integrated. Without delving into the actual instruments of manipulation, an attempt was made to visualize all progress as a series of activities.

Keywords: *Cybercrime, Hackers, Crackers, Cyberstalking, Child Solicitation and Abuse, Cyberterrorism, Sim Swap, Spammers, Combat, Mechanism, Cyber laws.*

*2nd year BA. LL.B. (Hons); student of Central University of South Bihar, GAYA; Available at: aryan.mitali1710@gmail.com

INTRODUCTION

Cyber crime refers to any illegal act that uses a computer, network device, or network. While most cybercrimes are typically used to make cybercriminals profitable, some of these activities are carried out to degrade performance, or directly disable the device or other computers, or to spread malware using other devices to obtain access to infect information, images or other materials illegally through targeted attacks on computers with the virus, which spreads to other devices and spreads through the network.

Information security is not an issue as cybersecurity specialists are on the lookout. With organizations that depend on IT, board members are more concerned with information security, as this potential threat can affect business and financial goals. The leaders of public institutions, including society as a whole, share the same concern. Information technology affects people, companies, public institutions and society, and we must adapt. Society as a whole is vulnerable to security incidents Institutions that are vulnerable to attack, such as military units, security agencies, nuclear reactors, etc. In a digital global society there are no borders, so cyberattacks can target any target, no matter what target is where you are. The global economy is made up of commercial networks that connect different companies to each other and, in many cases, make companies dependent. A cyber attack on one of the several companies in this chain could affect the entire economic group.

Cyberattacks are becoming more widespread and therefore have a huge impact. Cybercriminals are constantly developing new and ingenious ways to get onto networks. To this end, IT security professionals must be proactive and preventive in increasing the security of their systems. As cybersecurity attacks become more sophisticated, companies respond by strengthening their defenses. The recurrence and seriousness of digital assaults is expanding. Cybercriminals invest in Internet security solutions through a prioritization system and cost-benefit analysis. Proactive consideration by security experts, as well as ever-increasing financial investments in security solutions, appear to be the driving force behind success.

STATEMENT OF PROBLEM

From above, it is obvious that there are loopholes in cyberspaces, making it the obvious cause of most cybercrime. Thus, the following raises the issue:

1) The approach in which technology is exploited by individuals and the masses known as cybercriminals has intensified the impact of cybercrime on global security. These people have mastered the ability to use computer networks to their advantage. They commit crimes such as data breaches, hacking, spying, and spreading viruses while hiding behind computer screens. Almost most nations have well-developed Internet networks. The industry has advanced lately as large telecommunications companies struggle to roll out 5G networks around the world.

2) However, there is concern that criminals may use this network to gain access to the information systems of victims' organizations, which could lead to destruction and loss on all continents. Criminals in the 21st century employ a variety of methods to attack sensitive data, resulting in the highest cases of fraudulent activity on record to date. Victims lose confidential information, money, and even their identities to cybercriminals. This research aims to examine the different types of cybercrime that have shaken the world in the new millennium. The study also aims to examine the impact of such activities on international security and, consequently, the measures necessary to solve the problem.Research Questions:

The following questions are the concern of this research:

1. What are the various sorts of cybercrime that cybercriminals have utilized over the most recent twenty years?
2. What influence does cybercrime have on the globe and international security?
3. What are the reasons that are letting cybercrime grow rapidly?
4. What steps can the world community take to bring the situation under control?
5. How is the PDP Bill effective in combating the cybercrime?

RESEARCH OBJECTIVES

1. This research aims to identify the different types of cybercrime that have been used by criminals in recent years.

2. The objective is to examine how cybercrime has affected the world and international security.

3. The purpose of this document is to examine the main reasons that have supported the rapid growth of cybercrime.

4. Try to equalize the world community and take all necessary measures to alleviate the situation.

5. The document also analyzes how the Personal Data Protection Law is effective in regulating cyber crime.

TYPE OF STUDY

The researcher has chosen a descriptive and explanatory study form that corresponds to the topic, an adequate description was elaborated through an analytical approach with the help of laws, statutes, cases.

LITERATURE REVIEW

1. Mohammed I. Alghamdi, 2020, A descriptive study on the impact of cybercrime and possible measures to stop its worldwide spread, INTERNATIONAL JOURNAL OF RESEARCH AND TECHNOLOGY IN ENGINEERING (IJERT) ISSN: 2278-0181 Volume 09, Number 06 (June 2020);

Recently, a great deal of scientific work has been done to try to define cybercrime at different stages of history and in different situations. Cybercrime is defined as a harmful activity carried out by or against a system or network as established by the International Journal for Information Science and Security. Bernik (2014) characterizes cybercrime as "criminal operations completed by electronic activities determined to assault PC frameworks and information handled by the gadgets".

The 21st century was marked by important technological advances that have influenced human interaction. A digital age that has spread throughout the world has improved the social, political and economic facets of human life. The use of computers and electronic devices has increased dramatically around the world. These changes have led to a significant increase in crime, especially in virtual worlds. Cybercrime has evolved over time, and attackers invent increasingly sophisticated methods every day. Despite the international nation's efforts to combat evil and limit its effects, cybercrime has increased at an alarming rate around the world. There are differences in the definition of cybercrime at the international level. While their definitions are not widely accepted, organizations such as the Council of Europe Convention on Cybercrime, the Convention of the League of Arab States, and draft conventions of the African Union have attempted to define cybercrime (Alazab & Broadhurst, 2015). Computer information is a word used in the Commonwealth of Independent States to characterize cybercrime. On the other hand, according to the agreement of the Shanghai Cooperation Organization, information crime is defined as the illicit use of the property of information. This article looks at the different forms and causes of cybercrime.

Different political groups and countries around the world understand the word cybercrime or cybercrime differently. As a result, not all cybercrime is treated or criminalized equally in all states. This means that cybercrime can be considered a crime in one country but not a crime in another. The terms cybercrime and cybercrime are used interchangeably in this investigative report to refer to any crime that uses computer data and systems or is aimed at committing an illegal act.

2. UNITEDNATIONS:OFFICEONDRUGANDCRIME-COMPREHENSIVESTUDYONCYBERCRIME

In accordance with paragraph 42 of the Salvadoran Declaration on Comprehensive Strategies for Global Threats, the General Assembly proposed that the Crime Prevention and Criminal Justice Commission maintain: An open panel of experts on governments, crime prevention and criminal justice systems and Its advancement in a digital world, becomes a comprehensive study of the mystery of cybercrime and responses to it by member countries, global organizations and the business sector, including the exchange of information on national laws, methods, technical assistance and global cooperation with the objective of analyzing decisions to improve the suspension of a judicial system.

Cybercrime, authoritative reactions to cybercrime, wrongdoing counteraction and criminal equity limit and different reactions to cybercrime, global associations, and specialized help were a portion of the points considered for a complete investigation of cybercrime. Twelve subtopics were created from these main topics. 3 These topics are covered in eight chapters of this study: (1) cybercrime and connectivity; (2) The bigger picture; (3) regulations and framework conditions; (4) criminalization; (5) law enforcement and inspections; (6) digital evidence and the justice system; (7) International Coalition; and (8) prevention. The information was provided by 40 companies in the business sector, 16 academic institutions and 11 intergovernmental organizations. The secretariat also evaluated around 500 open source materials. Appendix 5 of this study provides more methodological information.

The United Nations Office on Drugs and Crime was commissioned to develop the study methodology, which included the creation of a data collection questionnaire, data collection and analysis, and the writing of the study text. From February to July 2012, UNODC carried out data collection according to the methodology, including the distribution of a questionnaire to Member States, intergovernmental organizations, representatives of the business sector and academic institutions. Information was provided by 69 Member States, broken down by region as follows: Africa (11), America (13), Asia (19), Europe (24) and Oceania (25) are the top five continents.

The study provides an overview of crime prevention and criminal justice initiatives aimed at preventing and combating cybercrime at a specific time.

Provides a complete picture by highlighting lessons from current and past efforts and outlining possible solutions for the future. Although the study is titled "Cybercrime," it is universally applicable to all crimes. It is difficult to unravel a "cyber crime" or even a crime that does not have electronic evidence of Internet connectivity as the world evolves into a hyper-connected society with universal Internet access.

SCOPE OF STUDY

Cybercrime can take several forms. The most common are described below:

1. **HACKING[1]:**This is a type of criminal act that involves breaking into someone's computer to gain access to personal or confidential information. This is different from ethical hacking, which many companies use to test their Internet security protection. In the hacking system, the criminal uses an assortment of programming to enter an individual's PC and the individual may not understand that their PC is being gotten to from a distant area.

2. **THEFT:**Crime occurs when someone violates copyrights and downloads music, movies, games, and software. There are even peertope websites that promote software piracy, and the FBI is currently investigating several of these websites. Today, the court system fights cybercrime and there are rules that prohibit unauthorized downloading.

3. **CYBERSTALKING[2]:** This is a type of online stalking in which the victim is bombarded with messages and emails online. These stalkers often know their victims and use the Internet to do so rather than personally following them. If they find out that online bullying is not having the desired effect, in addition to cyber bullying, they will start doing it offline to make the victims' lives even more pathetic.

4. **MALICIOUS SOFTWARE:**Refers to Internet-based software or programs that are designed to cause network disruptions. The software is used to access a system for the purpose of stealing confidential information or data or damaging the software of the system.

5. **IDENTITY THEFT:** As more and more people use the Internet for monetary transactions and banking services, it has become a serious problem. In this cyber crime, a criminal obtains information about a person's bank account, credit cards, social security number, debit card, and other confidential information to extract money or buy

[1] Arindam Sarkar: A Seminar Report on Cybercrime; Available at: https://www.slideshare.net/ArindamSarkar9/cybercrime-a; (Last visited on 9th October,2021 at 11:54 AM IST)

[2]Ibid

items in line with the identity of the victim. It can result in significant financial loss for the victim and potentially corrupt the victim's credit history.

6. **CHILD SOLICITATION AND ABUSE:**This is another type of cybercrime where criminals track teens through chat rooms looking for child pornography. The FBI has monitored chat rooms frequented by teens to help contain and prevent child abuse and advertising.

7. **CYBER-TERRORISM:**The severity of cyber terrorism distinguishes it from other types of white collar crime or hacker attacks. According to the testimony of Professor Dorothy Denning of Georgetown University, cyber-terrorist attacks on computer networks or the information stored on them must "result in violence against people or property, or at least cause enough damage to create fear." "Strikes that affect non-essential services or that are primarily a costly nuisance" are not classified as cyberattacks by definition

THE PERPS – HACKERS AND THE CRACKERS

HACKERS:

A hacker is defined as "a technician who intends to gain unauthorized access to the system system." Under Section 66 of the IT Act 2000, a hacker is any person who destroys, deletes or alters the information contained in a computing resource, or reduces its value or usefulness, or is adversely affected in any way, with the intention to cause it or knowing that it is capable of doing so. to cause unlawful loss or damage to the public or any person.

CRACKERS:A "cracker" is a hacker who has the intent to commit a crime. According to Search security techtarget.com[3], this term is used to distinguish "benign" hackers from

[3] Techtarget Network Search security; Available at: https://searchsecurity.techtarget.com/definition/cracker#:~:text=hacker&text=The%20Glossary%20defined%20a%20computer,for%20breaking%20into%20a%20system.%22; (Last visited on 5th October,2021 at 13:08 PM IST)

malicious hackers who damage target machines. Hackers deliberately destroy computers, steal information from secure networks, and disrupt connections for personal or political gain.

WHY DO PEOPLE HACK?

Cybercrime is defined as a "new way of tackling" new types of crime, much higher levels of crime and victimization, the need to react much more quickly, and enormous technological and legal complexity. As a result, hackers may be motivated by personal, political, or professional reasons.

EMPLOYEES: According to one study[4], disgruntled employees are the number one threat to computer security. In exchange for financial gain, employees steal confidential information and trade secrets. Angry insiders are one of the leading causes of cybercrime, according to CBI (Cybercrime Cell). Insiders don't need a deep understanding of their target systems, as their inside knowledge gives them unfettered access to damaging or stealing data from the user's system.

RECREATIONAL HACKERS[5]: For the thrill of defiance or self-aggrandizement in the hacking community, "recreational hackers" disrupt computer networks. With little experience with the attacked systems, the recreational hacker downloads the attack script and logs from the Internet before launching them on the victim's website.

WEBSITE ADMINISTRATORS AND THE WEB PAGES: Websites also have access to a variety of hidden background information from the user. The remote website can access the following critical visitor information:

1. The user's IP address;
2. birth number and dates of previous visits to the website;
3. The URL of the page that contained the link that led the user to the website;
4. The type of browser and the operating system and version of the user;

[4] Neelesh Jain and Vibhash Srivastava's "CYBER CRIME CHANGING EVERYTHING – AN EMPIRICAL STUDY"; Available at: https://www.researchgate.net/profile/Neelesh-Jain-3/publication/275709598 (Last visited on 5th October,2021 at 12:20 PM IST)

[5]IBID; Last visited at 12:21 PM IST

5. The user's screen resolution;

6. If JavaScript and VBScript are enabled on the user's computer; grams How many web pages the user has visited; hours the local date and time;

7. FTP username and password.

CYBERCRIME-CASE STUDIES

Following are the list of famous cases that happened around the world:

1) **PERIL TO CYBERBANKING IN SOUTH[6]:**

Most banks in South Africa process their customer data with mainframes. Using a mainframe relies on the computer's ability to perform a large amount of data processing autonomously, rather than having many computers processing small amounts of data.

Virtualization, which makes it easy to develop many logical computers within a single mainframe to work together, is another advantage of mainframes. Due to robust design and components, mainframes are typically larger than servers, allowing for multiple availability zones and versatility. Many mainframe components, such as interface adapters and drives, can be changed or upgraded without shutting down the server. When it comes to cybersecurity, banks face the following challenges:

1. System downtime
2. Customer data protection
3. Industry call
4. Critical infrastructure protection

[6] P. N. V. Kumar, "*Growing cyber crimes in India: A survey*," 2016 International Conference on Data Mining and Advanced Computing (SAPIENCE), 2016, pp. 246-251, doi: 10.1109/SAPIENCE.2016.7684146. Available at: https://ieeexplore.org/document/7684146 last visited 4th October,2021(Last visited on 5th October,2021 at 1:20 AM IST)

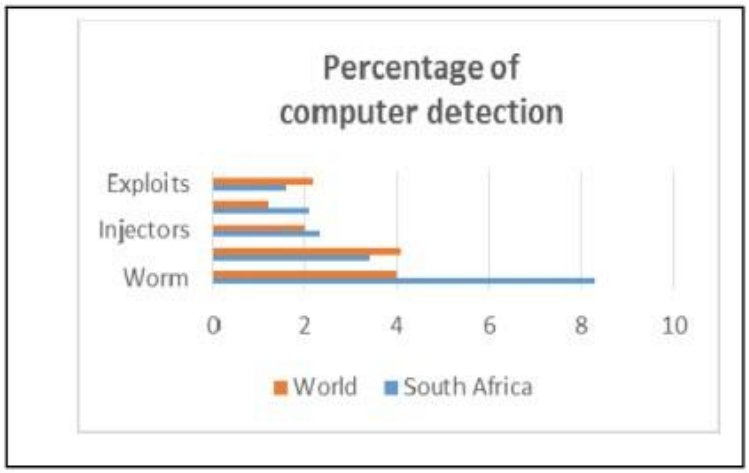

Fig 2: The Microsoft Security Intelligence of 2014 – South Africa

Due to inadequate security measures, cyber crooks often target less developed countries and then use this exploitation to attack more developed countries in order to gain access to large multinational corporations. Cybersecurity across the country could be at risk if cyber banking security is breached. As a result, there have been some serious violations [6]. In January 2016, Check Point, a security organization, identified South Africa as one of the most vulnerable countries for cyber thieves. In January 2016, South Africa went from 67th to 22nd on the threat cloud map of the countries most targeted by cyber thieves. According to Check Point, 4,444 cyber fraud attempts targeting video-on-demand customers escalated, misleading consumers into providing private credentials that they believed their accounts needed to be updated. Spam emails with attachments containing malware on users' systems are widely used for phishing attacks. Viruses, worms, and other exploit software are examples of malware. To gain access to secure information or resources, today's malware tries to copy data from one area to another. 4,444 According to Symantec's February 2014 Intelligence Report, South Africa had the highest rate of phishing attacks in February 2014, with one in 668 emails identified as suspected of phishing fraud. Furthermore, spam was detected in one out of every two emails in South Africa. South Africa ranked seventh among the top ten phishing sources and first among the top five phishing destinations geographically. Between January and June 2012, the RSA AntiPhishing Service in South Africa recorded a total of 1,942 new phishing attacks with a potential net loss of approximately $ 6,828,072. 4,444 worms were the most common type of malware, according to Microsoft's Security Intelligence Report, and 8.3 percent of PCs in South Africa were infected in the fourth quarter of 2014. Since the third quarter of 2014 there was a decrease 10.2 percent [6]. Trojans and obfuscators and injectors were the second and

third most common malware in South Africa. From 4.9 to 3.4 percent and from 2.7 to 2.3 percent. The most common category was Potentially Unwanted Software, which came in second. About 30% of all computers cleaned belonged to this group. Adware ranked third on the list and affects nearly 19 percent of systems handled in South Africa. To combat the rise in cybercrime, the South African government has enacted laws, guidelines, and regulations.

1. **MECHANISMOFPREVENTION**[7] – Proposition of a structure that utilizes a validation/approval technique just as a firewall to give line security to the financial area. The firewall would be arranged to channel network traffic dependent on the data in the parcel header. The arrangement head is liable for characterizing and dealing with this information.

2. **INFORMATION ABOUT CREDIT AND DEBIT CARDS ARE STOLEN[8]:**

In 2007, three men were charged with hacking cash registers and collecting data from thousands of credit and debit cards at Dave & Buster restaurants in the United States. That information was later sold, resulting in a loss of more than $ 600,000. One from Ukraine and the other from Estonia hacked into payment machines at 11 Dave & Buster locations and installed "trackers" to steal payment information sent from point-of-sale terminals to company headquarters. Later, at TJMax, the same men were charged with a similar crime. Some analysts forecast TJ Max's losses of more than $ 1 billion. One of the three men was accused by a US Postal Inspection Service inspector of being a major reseller of stolen ID cards. The three children were arrested while visiting two countries that are actively working with law enforcement agencies in the United States, Turkey and Germany, and not at their homes in Eastern Europe.

[7] P. N. V. Kumar, "Growing cyber crimes in India: A survey," 2016 International Conference on Data Mining and Advanced Computing (SAPIENCE), 2016, pp. 246-251, doi: 10.1109/SAPIENCE.2016.7684146. Available at: https://ieeexplore.org/document/7684146 last visited 4th October,2021 at Last Visited: 5th October 2021, 1:46 AM IST

[8] Lingaraj, Haldurai. (2014). *A Study on Cyber Crime*. Available at: https://www.researchgate.net/publication/274713543_A_Study_on_Cyber_Crime (last visited: 5th October,2021 at 01:59 AM IST)

3. DDOS ATTACKS BY BLUE SECURITY[9]:

Blue Security, an anti-spam company based in Israel and California, was founded in 2006. It has developed a novel way to combat spam. They would send requests to spammers asking them to stop spamming their consumers. This caused a lot of headaches for spammers when they discovered that Blue Security was sending these messages on behalf of more than 500,000 customers, creating significant scalability issues. Although this vigilante virtual justice system was divisive by spammers, it appears to have been legal. The spammers returned the favor with a DDoS attack. Initially, Blue Security responded quickly and efficiently, but the scope and complexity of the attack escalated over time. Blue Security had no choice but to seek help from others. When Blue Security implemented Prolexic DDoS protection, which cleaned up their traffic, the spammers simply directed their DDoS attacks against Prolexis DNS and disabled them and many of their customers.

As a result, Blue Security was forced to go alone. As a result, the CEO eventually decided to close the company.

4. DDOS ATTACK ON NATIONAL AUSTRALIA BANK AND WESTPAC BANK[10]:

While Blue Security's DDoS attacks appear to have little to do with Australia, DDoS has been used as a retaliation technique on several occasions in Australia. The National Australia Bank (NAB) was hit by a DDoS attack in October 2006. According to law enforcement agencies, strikes have started in Russia. Then in September 2007, shortly after its new cybercrime response team was formed to tackle phishing attempts, Westpac Bank was hit by an attack with similar traffic patterns.

---

[9] T. M. Mbelli and B. Dwolatzky, "*Cyber Security, a Threat to Cyber Banking in South Africa: An Approach to Network and Application Security*," 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud), 2016, pp. 1-6, doi: 10.1109/CSCloud.2016.18. Available at https://ieeexplore.ieee.org/document/7545887 ; (Last visited: 4th October,2021 at 14:02 PM IST)

[10] Lakshmanan, Annamalai. (2019). Literature review on Cyber Crimes and its Prevention Mechanisms. 10.13140/RG.2.2.16573.51684. Available at: https://www.researchgate.net/publication/331010726_Literature_review_on_Cyber_Crimes_and_its_Prevention_Mechanisms. (Last visited on 4th October,2021 at 20:15 PM IST)

5. **SIM SWAP FRAUD[11]:**

Two people from Mumbai were arrested for cybercrime in August 2018. They have been involved in fraudulent money transfers from various people's bank accounts after illegally stealing their SIM card information. These scammers obtained people's personal information and then used fake documents to block their SIM cards and subsequently made transactions through online banking. They were accused of illegally transferring Rs 4 million from many accounts. They even tried to hack the accounts of some companies. In this case, scammers access consumer information such as phone number, name, proof of identity, and other details of an organization or a public area. After that, they acquired a 4G SIM card by providing the telecommunications company with the required data of customers who had previously used a 3G SIM card, as well as their phone numbers, and then they called the consumer and acted as customer service agents. . They provide the consumer with a 20-digit code that is written on the back of the 4G SIM card and ask them to quickly enter and activate the 4G SIM card. People who do this have their 3G SIM card removed and their 4G SIM card activated. However, scammers continue to use 4G SIM cards to bank and obtain OTP.

MECHANISM OF PREVENTION[12]-

Sharing personal information with unfamiliar applications and domains can reduce the chance of one`s personal information being accessed by those who are malevolent. In a variety of scams, fraudsters use the victim`s information to dupe them into participating in fraudulent activity. As a result, it is recommended that the site where an individual enters his or her banking or other personal information be checked for legitimacy, as scammers utilize bogus sites to obtain information directly from potential victims. Customers are also needed to activate the sim card if it is physically present with them.

[11]Ibid

[12]Supra note of 12

CYBER ATTACK ON COSMOS BANK[13]-

In August 2018, a daring cyberattack on Cosmos Bank`s Pune branch resulted in the theft of over 94 crore rupees. By compromising Cosmos Bank`s server, hackers were able to wipe out money and move it to a bank in Hong Kong. Cosmos bank has filed a cyberattack case with the Pune cyber cell. Hackers gained access to the bank`s ATM server and stole the personal information of numerous Visa and Rupay debit cardholders. The hack did not target Cosmos Bank`s centralized banking solution. Balances and total account information were unchanged, holders' bank accounts were not affected. The goal was to create a switching system that serves as a communication link between the payment gateways and the bank's centralized banking solution. The malware attack on the switching system resulted in a series of false signals verifying various Visa and Rupay debit card payment requests from around the world. The total number of transactions was 14,000, with more than 450 cards used in 28 countries. 400 cards were used with a total of 2,800 transactions nationwide. This was India's first malware attack on the switching system that caused the payment gateway and the bank to go offline.

MECHANISM OF PREVENTION[14]-

The way forward could be to strengthen security systems by limiting their functions and performance to only authorized users. Any illegal access to the network must be reported immediately and all access to the bank's network must be blocked. Enabling two-factor authentication can also help reduce risk. Possible weaknesses can be discovered through tests, whereby the security of the entire digital banking system is ensured.

[13]Cosmos Bank malware attack: Interpol issues red corner notice against prime suspect traced in foreign country, published in Indian Express.com; Available at: https://indianexpress.com/article/cities/pune/cosmos-bank-malware-attack-interpol-issues-red-corner-notice-against-prime-suspect-traced-in-foreign-country-6574097/; Last visited on 5th October,2021 at 10:27 AM IST.

[14] Testbytes.net. (2018). Major Cyber Attacks on India (2018) - Testbytes. Retrieved August 23, 2018; Available at: https://www.testbytes.net/blog/cyber-attacks-on-india/ ; Last visited on 5th October,2021 at 11:20 AM IST.

CHALLENGES AHEAD

The challenges of the digital age and the investigation of electronic crime, cybercrime or cybercrime are diverse and include:

1. Crossing multiple jurisdictions;
2. Preserve and preserve evidence;
3. Obtaining appropriate powers;
4. Decoding encryption
5. Proof of identity;
6. Know where to look for evidence;
7. Rethink costs and research priorities;
8. Crime response in real time;
9. Coordination of research activities;
10. Improve training at all levels of the organization;
11. Development of alliances and strategic alliances;
12. Improvement of electronic crime reporting;
13. Improvement of the exchange of information and messages;
14. Acquisition and develop and retain specialized personnel and avoid "technological lag" (or obtain access to cutting-edge technology).

Forensic challenges in particular are too great. The US Department of Justice Identified Four Major Challenges in Gathering and Analyzing Forensic Evidence in a Report (2001, p.23)[15];

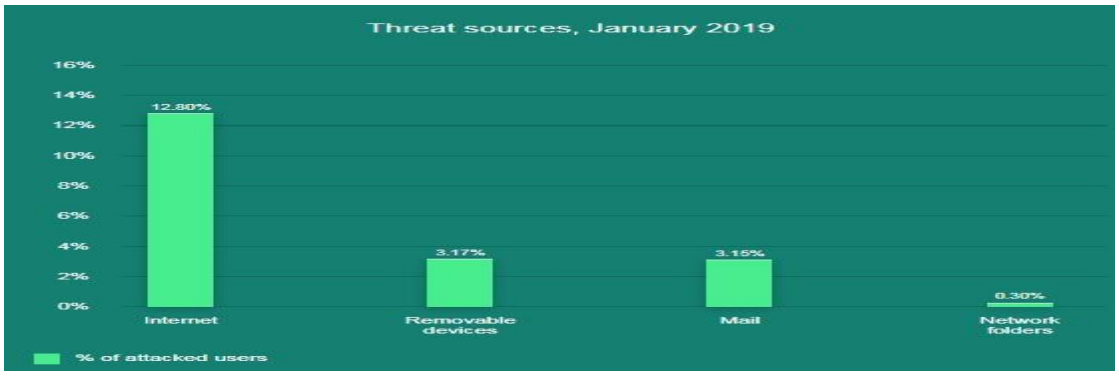

Figure: 2 Threat sources vs % of attacked users

[15] Neelesh Jain and Vibhash Srivastava's "CYBER CRIME CHANGING EVERYTHING – AN EMPIRICAL STUDY";Available at: https://www.researchgate.net/profile/Neelesh-Jain-3/publication/275709598_CYBER_CRIME_CHANGING_EVERYTHING_-_AN_EMPIRICAL_STUDY/links/554493760cf23ff7168546c5/CYBER-CRIME-CHANGING-EVERYTHING-AN-EMPIRICAL-STUDY.pdf; (Last visited on 5th October,2021 at 13:40 PM IST)

Algeria, Morocco, Egypt, Vietnam and Indonesia are the five countries with the highest proportion of attacks in January 2019. In January 2019, the total proportion of infected industrial computers was around 22.3 percent. The sources of threat and the proportion of industrial computers attacked in January 2019 are shown in the graph.

• Finding relevant evidence in the "Information Ocean": It can be difficult to find relevant evidence in the "Information Ocean". Separating valuable xz1 1232 data from irrelevant data also requires considerable technical effort. Finding where to save your evidence can also be tricky.

• Anonymity: People can easily remain anonymous on computer networks, and most web servers have a fictitious "identifier", name or identity.

• Traceability: anonymity refers to traceability, which indicates how difficult it is to determine the origin and destination of messages on computers and communication networks such as the Internet. The development and easy availability of various communication providers make traceability even more demanding. For example, on the Internet, a message can easily be passed to ten different Internet Service Providers (ISPs), each of which must provide information to track it.

• Encryption - Most data and communications will be encrypted shortly. Due to the difficulty of cracking encryption, it can hamper police investigations and increase spending.

CYBER LAWS IN INDIA

One of the most important laws governing the administration of the Internet is the Information Technology Act of 2000 ("IT Act"), which interprets Internet security and protects against access, use, disclosure, interference, alteration or illegal destruction of information, devices and devices Computers, computing resources, communication devices and information contained in them. In addition to the legal recognition and protection of electronic data transactions and other forms of electronic communication, IT law and its regulations focus on digital security, defining adequate security standards for companies, redefining the role of intermediaries and recognizing the Computer Emergency Teams of India ("CERTIn"), among others. The IT Act also revised the scope of the IPC, the India Evidence Act of 1872, the Bankers Book Evidence Act of 1891 and the Reserve Bank of

India Act of 1934, and related matters. or complementary.[16], that we focus on extremely sensitive legislation in the banking and financial services sector. Although there is currently no general legislation for the governance of the data country, there are sectoral regulations, guidelines and legal recommendations that require specific compliance for the target sector.

The Information Technology Act applies not only to India as a whole, but also to any violation or violation committed by a person outside of India. Furthermore, the legal sanctions under the TI Act extend to incarceration, penalties and also provide a framework for the payment of damages to plaintiffs. The legal sanctions of the IT Law also include imprisonment, fines, and the creation of a compensation or redress structure for plaintiffs. When a company that owns, regulates or operates a computer resource that contains, processes or manipulates private information or sensitive information or details, it is negligent in implementing adequate security procedures and therefore causes an individual an illegal loss or gain, as the company is subject to compensation and remuneration.

CERTAIN SIGNIFICANT REGULATIONS ENCOMPASSED PINNED IN THE INFORMATION AND TECHONOLOGY

The Indian Computer Emergency Response Team and Art of Performing Duties and Duties Rules 2013 ("CERT Rules") govern information technology.

CERTIn was established as the central body in charge of collecting, analyzing and disseminating information on cyber threats and of taking emergency measures to control such incidents in accordance with CERT standards. In addition, these rules require reporting to CERT in the following situations:

(i) intentional invasion or violation of critical networks or systems;

(ii) unapproved admittance to IT frameworks or information;

(iii) Website tampering, malicious software attacks, denial of service and distributed denial of service (DDoS) attacks, and attacks on domain systems of the website and related services are examples of crimes cybernetic; and

[16] Shubhangi Agarwal Lexology Cyber security in India TMT Law Practice; Available at:https://www.lexology.com/library/detail.aspx?g=d7b0a465-cc55-48e9-9534-b05bf0c036bd; (Last visited on 6th October,2021 at 22:07 PM IST)

(iv) electronic administration and electronic commerce are two examples of applications that have been addressed. Individuals and businesses can also report additional cyber incidents or breaches to CERTIn and receive the necessary professional support and assistance to help them recover. Unfortunately, the information requirements of the law are insufficient and therefore need to be reviewed as they are voluntary rather than necessary. This eliminates the need for companies to maintain the transparency they need.

Data Technology Rules (Appropriate Security Practices and Procedures and Sensitive Personal Data or Information) 2011 (the "SPDI Rules").

These SPDI rules strictly regulate companies collecting and processing sensitive personal data in India. The rules (i) require consent to collect information; (ii) insist that it is only for a legal purpose; (iii) require organizations to have a privacy policy; (iv) give instructions on data retention; (v) grant people the right to correct their information, and (vi) impose restrictions on the disclosure, data transfer and security measures. In addition, certain sectors such as banking, insurance, telecommunications, health, etc. They have data protection provisions in their respective sectoral regulations. In the absence of more extensive or stricter legislation, the existing framework at least complies with basic data protection principles and offers companies more leeway to adopt current standards and best practices for the respective industry.

THE PERSONAL DATA PROTECTION BILL 2019

The Personal Data Protection Bill 2019[17] ("PDP Bill"), a fresh version of data privacy and protection legislation, was introduced in December 2019. Section 24 of the PDP Bill requires data fiduciaries (also known as "data controllers") to put in place safeguards for a variety of reasons, including preventing misuse, unauthorized access to, modification, disclosure, or destruction of personal data. Section 25 also addresses data breaches. According to the clause, if a data breach poses a risk of harm to the data principal, the data fiduciary shall notify the proposed Data Protection Authority.

[17] Angelina Talukdar's "Article on INDIA: Key Features of the Personal Data Protection Bill, 2019; Available at: https://www.mondaq.com/india/data-protection/904330/key-features-of-the-personal-data-protection-bill-2019; (Last visited on 8th October, 2021 at 09:45 AM IST)

In response to growing concerns about privacy and cybersecurity, the government is evaluating dangers (including political opportunities), and restrictions on vulnerable populations (children) and highrisk apps (including ecommerce platforms) have been implemented.

INTERCONNECTED WORLD: CYBERCRIME PREVENTION

The oppressive reliance of the corporate world on Zoom, which resulted in a large number of people rushing into 'office meetings/ Zoom parties,' disturbing the flow of a particular session, is one of the most pertinent references of these times that can be made in the current circumstances. Individuals and businesses are increasingly moving away from the platform and toward [supposedly] tougher platforms for work-related calls. In the aftermath of this cyber-threat, even intergovernmental entities like the European Commission have turned away from Zoom for work-related calls[18].

Obligations of Data Fiduciary[19]:

The processing of personal data is subject to specific purposes, collection and storage restrictions, such as:

1. For a specific, clear and lawful purpose.
2. The collection of personal data is limited to the data that is necessary for the purposes of the processing.
3. The collection or processing of personal data must be communicated to the person / data controller.
4. Personal data is only stored for the purpose for which it was processed and is deleted once the processing is completed.
5. At the beginning of the data processing, the consent of the person responsible for the treatment must be obtained.

[18] Shubhangi Agarwal Lexology Cyber security in India TMT Law Practice; Available at:https://www.lexology.com/library/detail.aspx?g=d7b0a465-cc55-48e9-9534-b05bf0c036bd; (Last visited on 7th October,2021 at 15:00 PM IST)

[19]*Section13 defines "Data Fiduciary" as any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data.*

6. The data administrator must verify age and obtain parental consent when processing sensitive personal data of children.

In addition, data trustees must comply with certain transparency and accountability obligations, such as: (i) preparing a data protection policy, (ii) taking the necessary measures to maintain transparency in the processing of personal data, (iii) take security precautions (for example, data encryption and prevention) misuse of data), (iv) report to the authority notifying any breach of any personal information (v) review their policies and implementation of policies each year, (vi) conduct a data impact assessment if a key data manager performs data processing involving new technology or sensitive personal information (vi) important data The manager appoints a protection officer of data to advise and supervise the activities of the data administrator , and (vii) establish complaint procedures to resolve er complaints from individuals to edit.

Data Protection Authority: The bill proposes that an Indian data protection agency take steps to protect people's interests, prevent misuse of personal data, and ensure compliance with the bill and promote privacy awareness. The authority's decisions can be appealed to the appellate court. The court's decision can be appealed to the Supreme Court.

Restrictions on Transfer of data outside India: Sensitive personal data may be transferred outside of India for processing if the person has given their express consent and under certain additional conditions. However, this sensitive personal data must be stored in India. Certain personal data reported by the government as Critical Personal Data can only be processed in India.

Exemptions[20]: The central government has the power to exempt any government agency from the applicability of the law if this is necessary to:

i. Interest in the sovereignty and integrity of India, the security of the state and friendly relations with foreign states,

[20] Angelina Talukdar's "Article on INDIA: Key Features of the Personal Data Protection Bill, 2019; Available at: https://www.mondaq.com/india/data-protection/904330/key-features-of-the-personal-data-protection-bill-2019; (Last visited on 09th October, 2021 at 12:44 PM IST)

ii. prevent the incitement to the commission of a crime typified in the penal code in relation to the aforementioned matters.

The processing of personal data is also exempt from the provisions of the bill for other purposes, such as: (i) prevention, investigation or prosecution of criminal offenses, or (ii) personal, domestic or (iii) journalistic purposes, (iv.)) For statistical or research archiving purposes.

Risk of non-compliance with PDPB[21]: There are two penalties and compensations:

i. Failure to comply with the data protection obligations of the data administrator can result in a fine of up to Rs 5 billion or 2% of your total worldwide sales for the previous financial year, whichever is greater.

ii. Processing of data in violation of the provisions of the PDPB will result in a fine of 15 million rupees or 4% of the annual turnover of the data administrator, whichever is greater.

The recognition and processing of anonymized personal data without consent is punishable by imprisonment of up to three years or a fine or both.

[21]Supra note of 22

CONCLUSION

Cyberspace violation is a fight we fight on a daily basis. India needs strict laws and guidelines to combat these problems. The existing legal framework does not adequately address the concerns of the sector and there is an immediate need for comprehensive legislation to address these concerns.

A proactive approach must be developed by CIOs and senior management to increase information security. IT risks are no longer just a technical risk in the CIO area; it is also a business risk that must be addressed along with all other material risks.

As we decide to stay in touch, we will discuss expanding and acquiring large data sets that are integrated (data warehousing, deep learning, AI, Internet of things); This exposes the entire ecosystem to greater threats from social deviants. Individuals and corporate bodies are responsible for maintaining the security and integrity of data while ensuring that access to data is not compromised in any way. Healthcare, banking and financial services companies rely on their own technology and organizational security protocols to ensure that data is not corrupted or prone to inappropriate and unauthorized access despite upcoming legislation. The insurance business supports the lack of an effective legal system by encouraging preventive care for businesses and individuals. Cybersecurity insurance has gained enormous popularity, compounding the lack of an effective legal system.

Following the enactment of the PDPB, companies that process personal data must meet a number of requirements to protect the privacy of individuals in relation to their personal data.

Individual consent would be required for the processing of personal data. Organizations should review and update privacy policies and codes based on the type of personal data being processed to ensure they are in line with the revised principles.