CYBERSECURITY AND LEGAL RAMIFICATIONS: AN IMPORTANT CONCERN IN INDIA

Tanmay Vashishta, UPES, School of Law

ABSTRACT

It's difficult to imagine life in today's world without the internet, and it's no surprise that it's become one of the most popular and essential outlets for not only e-commerce, but also education, work, and even gaming. With the growth of the internet came the concepts of cyberspace, cybersecurity, and cyber-attacks. Internet security is not taken seriously in India, which has led to an increase in cybercrime. Even if many of us take precautions to secure our data and ourselves, someone monitors what we upload and download to and from internet outlets without our knowledge. And it is here that the practice of cybersecurity is put to its best use. As technology advances, there has been an increase in the production of newer models and trends in cyberspace and cybersecurity to meet the increasing demands. The rule that regulates the entire cyberspace and all of its components is known as cyber law. It defends against cybercrime and imposes penalties on those who break it. Cyberlaw refers to the legal authority and control of different aspects of the internet and computer security.

On the other hand, cybersecurity law is described as "a new emerging legal discipline within the cyber law umbrella that deals with all legal policy and regulatory issues relating to cybersecurity, its defense, preservation, maintenance, and continued advancements. In the ongoing growth of information technology and Internet services, cybersecurity plays a crucial role. Enhancing cybersecurity and safeguarding sensitive information infrastructures are critical to the security and economic well-being of every country. Cybersecurity is critical for reducing cybercrime and protecting victims. Cybercrime is managed by cybersecurity. "Cybercrime victims can help to reduce cybercrime risk. Cybercrime is combated by cybersecurity

INTRODUCTION

Cybersecurity is a technique for preventing unauthorized access and threats to computers, networks, utilities, and personal information. It is the process of protecting and defending information and other communication networks from unauthorized access, modification, or exploitation. Cybersecurity is also known as information technology defense. It addresses methods for protecting computers, networks, facilities, and data from unauthorized access or attacks that could damage or exploit them somehow. In essence, cybersecurity is a technical solution to safeguarding networks from such attacks. Cybersecurity considers all of a computer system's or network's weaknesses and risks. It then determines the root cause of such flaws, corrects the flaws and risks, and secures the system. Cybersecurity systems that are successful combine technical and human elements. According to the IT[1] Act, 'cybersecurity' refers to protecting information, equipment, devices, computers, computer resources, communication devices, and the information stored on them from unauthorized access, usage, disclosure, disturbance, alteration, or destruction. The National Cyber Crime Reporting Portal[2] (a government-created body set up to promote reporting of cybercrime complaints) defines 'cybercrime' as "any illegal act in which a computer or communication system or computer network is used to commit or facilitate the commission of crime.'

SIMILARITIES BETWEEN CYBERCRIME & CYBERSECURITY

- **Cybercrime**: Cybercrime is a form of criminal activity that involves the use of computers and the Internet. It can be perpetrated against a single person, a group of persons, the government, or a private company. It is usually done to damage someone's reputation, inflict physical or mental harm, or profit from it, such as monetary gain, spreading hate and fear, and so on. The core concept of cybercrime law is to prosecute unauthorized access to or unlawful use of computer systems and the internet with malicious intent to prevent harm and modification to such systems and data. On the other hand, cybercrime poses the greatest danger to an individual's and the government's financial security.
- **Cybersecurity**: The value of cybersecurity is increasing. Fundamentally, our world is more technologically dependent than it has ever been, and this development shows no signs of slowing. Data breaches that could lead to identity fraud are now being shared

[1] The Information Technology Act, 2000
[2] https://cybercrime.gov.in/

openly on social media pages. Social security numbers, credit card numbers, and bank account records are now stored in cloud storage services such as Dropbox or Google Drive. If you're a person, a small company, or a large corporation, you depend on computer systems daily. When you combine this with the proliferation of cloud computing, insecure cloud services, smartphones, and IoT[3], you have a slew of cybersecurity risks that didn't exist only a few decades ago. Even though the skillsets are becoming more similar, we must consider the difference between cybersecurity and information security.

VARIOUS ASPECTS OF CYBERSECURITY

- **Application protection:** Since applications are so important in business, every company should pay attention to web application security. Customers, their knowledge, and their interests are all protected by web application protection. Application protection assists in thwarting any attempts to circumvent the authorization limits imposed by the operating device or network's security policies.
- **Information Protection:** Information includes corporate records, personal data, consumer data, intellectual property, and so on; thus, a company needs to have good cyber security to avoid information leakage. Information security refers to protecting sensitive data from unauthorized access, use, or harm of some kind. This also guarantees that critical data is not lost in the event of a natural disaster, device failure, fraud, or some other potentially damaging circumstance. Confidentiality, honesty, and availability are the attributes that define information security. Data Confidentiality, Data Privacy, Data Availability, and Data Authenticity are all aspects of information security.
- **Network Security:** It refers to the protection of a network's accessibility and data's reliability. A network penetration test is used to evaluate a system's and network's security vulnerabilities. It describes a wide range of security policies for preventing and tracking unauthorized access, misuse, and damage to a computer device and other network systems. Network security encompasses a broad range of computer networks and private and public communication systems used by businesses and organizations.

[3] Internet of Things

- **BCP**[4]: Its' also known as 'Disaster Recovery', which is about being ready for any type of intervention or cyber threat by recognizing threats to systems promptly and assessing how they can impact operations and methods to counter the threat.
- **OPSEC**[5] :The term "OPSEC" refers to the safeguarding of an organization's functions. It locates critical data and properties in order to track down threats and vulnerabilities in the functional process.
- **End-user education**: Since human error is one of the leading causes of data breaches, businesses need to educate their workers about cyber security. Every employee should be aware of the most common cyber threats and be able to respond to them. Training will allow management to become familiar with system users and risks. In contrast, user training will aid in the elimination of resistance to change and advancements, as well as increased user scrutiny.
- **Leadership Dedication**: To have a successful cyber security program, organizations and companies must have leadership commitment. It is difficult to create, execute, and manage cyber security processes without a team leader.

CYBERSPACE & CYBERSECURITY

Cyberspace is a virtual computing environment with an interactive medium that connects the world's computers and allows people to communicate online. Cyberspace is a fictitious world where people communicate digitally. Individuals can use this global network to connect, exchange ideas, share knowledge, provide social support, perform business, direct actions, create creative media, play games, discuss politics, and so on. It is distinct from the internet, which is merely a medium, and cyberspace has its own separate life. With 462 million internet users and 200 million active Social Media users, India is the world's second-largest online economy, after China. Males account for 71% of users, while females account for 29%. The busiest hours are from 6 p.m. to 10 p.m., with the most Internet traffic coming from Mumbai and Delhi. The e-commerce market in India is the world's biggest. Furthermore, the Facebook App is now used by the majority of Indians around the world. Many other figures indicate that Indians use the Internet to a significant extent.

[4] Business Continuity Planning
[5] Operational Security

The above statistics and figures demonstrate the serious consequences of a violation of cybersecurity for Indian users. Contact numbers, email addresses, location detection, permission to use media, and other information requested by various apps and websites can compromise a person's privacy and security.

- **Characteristics in Cyberspace**

1) A land with no boundaries.
2) Interactive virtual Environment.
3) Unrestricted access.
4) It is found in nature.
5) Dissemination occurs at the same time.
6) The replication or duplication is as genuine as the original.

- **Information About Indian Cyberspace**

1) Internet connectivity is available to 45.15 percent of India's population.
2) India has the most Facebook users in the world.
3) After China, India has the world's largest online user base.
4) Internet traffic in Mumbai and Delhi is higher than in other cities.
5) In India, men outnumber women when it comes to internet use.

- **The Cyber World's Anatomy**

1) **The Surface Web:** (constitutes only 4 percent of cyberspace) The surface network includes Facebook, WhatsApp, and other social media and online websites.
2) **The Deep web:** (constitutes only 90 percent of cyberspace) It is usually not directly available, instead requiring the use of Ids and passwords. Medical records, legal papers, government archives, organization-specific directories, financial records, and other virtual information are examples of virtual information.
3) **The Dark web:** (constitutes only 6 percent of cyberspace) Pornography, illicit trade, and illegal drug trafficking through the silk route is all carried out in this space.

Cybersecurity's Emerging Trends and Developments

Enterprises often put privacy and protection first, whether it's when it comes to monetary transactions or employee details. According to a 2014 study, 98 percent of businesses have cybersecurity in place, and more than half are working to secure even higher quality and advanced protection steps. The majority of businesses that have taken cybersecurity seriously are planning for scenarios in which hackers may target them.

❖ CHALLENGES FOR CYBERSECURITY

- **Ransomware Evolution:** These attacks are one of the fastest-growing types of cybercrime in the economy. Ransomware[6] is the bane of cybersecurity, information technology, and data experts, as well as executives. Nothing is worse than malware that spreads and latches on to consumer and company data that can only be deleted if you comply with the cybercriminal's outrageous demands.
- **Malware Attack:** This is a general term that applies to various cyber threats such as Trojans, malware, and worms. Malware[7] is described as code written with the intent of stealing data or damaging something on a computer. Viruses infect other clean files by linking themselves to them. They can spread uncontrollably, causing harm to a system's key functions as well as the deletion or corruption of data. They are usually in the form of an executable file that you downloaded from the internet. Trojans, for example, is a form of malware that masquerades as legitimate software or is embedded in legitimate software and can be manipulated. It weakens your defenses by allowing other malware to penetrate through backdoors. On the other hand, Worms are whole networks of computers that use network interfaces to propagate locally or across the internet. With each infected device that follows it, it infects more computers.
- **Phishing:** is when someone pretends to be a third party and asks for information. Phishing emails are sent to users, requesting that they click on a connection and enter personal information. Phishing emails are often classified as spam, but they are much more dangerous than a typical advertisement.
- **Crypto-jacking:** It is the practice of using cryptocurrencies to make money. Crypto-jacking cases have increased in tandem with the growth of the cryptocurrency industry.

[6] https://www.itgovernance.co.uk/ransomware
[7] https://www.itgovernance.co.uk/malware-protection

Crypto-jacking is the practice of stealing computing resources from someone else's machine to mine for online currencies such as Bitcoin.

- **Attacks combining cyber and physical components:** It is only normal that knowledge about electric grids, dam structure and operations, water treatment, and transportation facilities be stored in cyberspace in an age where all is dominated by the internet. A breach in their security system has an immediate impact on real-time operations in an area, and if the breach occurs in the core system, it has an even greater impact on the entire nation. That is why they are known as cyber-physical attacks.

- **IoT Attack[8]:** It is a network of small digital devices such as cell phones, computers, and internet-connected devices such as modems, routers, and other internet-connected devices. Because of their nearly constant connection to the internet, IoT devices are more vulnerable to security breaches than any other system, allowing for easy open access to their data.

- **Password Attacks:** It's a general term for an attempt to access or decrypt a user's password for unauthorized purposes. For password attacks, hackers may use cracking programs, dictionary attacks, and password sniffers. Password cracking refers to a variety of techniques for deciphering machine passwords. Passwords are normally recovered from data saved in or transferred from a computer device. Password cracking is normally accomplished by repeatedly guessing the password using a computer algorithm that attempts various variations before the password is successfully discovered. Password attacks can be carried out for various purposes, the most malicious being to obtain unauthorized access to a device without the owner's knowledge. As a result, cybercrime emerges, such as the theft of passwords to gain access to financial data.
- **DDoS[9] Attacks:** The term is an acronym for "distributed denial of service It focuses on disrupting a network's service. Attacks send a large amount of data traffic across the network until it is overburdened and unable to operate. The attacker uses several computers to send traffic or data that overloads the device in a DDoS attack. An individual may be unaware that his or her machine has been hacked and is contributing

[8] Internet of Things
[9] Distributed Denial-of-Service

to a DOS attack in many cases. Disrupting services may have significant security and online access implications. Many large-scale dos attacks have been carried out as a single act of protest against governments or individuals, and have resulted in serious penalties, including lengthy prison sentences.

- **Man-in-the-Middle Attacks:** A man-in-the-middle attack obtains data from the end-user and the party with which he or she is interacting by impersonating the endpoints in online information exchange. If you're talking over the internet, for example, the man in the middle can communicate with you. By pretending to be you and communicating with your bank. The man in the center would then receive all of the data sent back and forth between the two sides, which may include confidential details including bank accounts and personal information.

- **Malvertising:** It is the term used in the security industry to describe illegally regulated ads that infect individuals and companies on purpose. These can be advertisements on any platform, mostly ones that people use as part of their daily internet usage, and it's becoming more of a concern, as shown by a recent US Senate study and the establishment of organizations like Confidence in Ads. These challenges can be monitored, and methodical measures can be taken to prevent such errors. Large technology companies should collaborate and develop solutions to improve consumer protection. Security measures must expand outward, starting at the application level, where frauds can be easily detected. Firms become vulnerable when there are no cohesive control methods in place.

CATAGORIES OF CYBERCRIMES

i. **Individual Crime:** Crimes against the person are those crimes committed against an individual's will to cause them physical or mental harm. Attack, harassment, kidnapping, and stalking are examples of crimes against individuals; but, in cybercrime, the scope of crimes against individuals varies slightly and includes cyber stalking, pornography, cyber bullying, child violence, fraud, and cyber threats. Cyber defamation, for example, is when someone uses the internet to damage another person's reputation. The following are a few examples of cybercrime perpetrated against individuals:

- Harassment in the form of e-mails.
- Dissemination of pornographic content
- Stalking on the internet.
- Defamation of character.
- Exposed indecently.
- Cheating is a serious offense.
- Unauthorized access to or control of a computer system.
- Email spoofing is when someone sends a fake email to someone else.
- The act of deception.

ii. **Theft of Property:** Cybercrime against property is the second form of cybercrime. With the expansion of foreign trade, companies and consumers increasingly turn to computers and the internet to develop, distribute, and store information in electronic form rather than conventional paper form. As a result, some cybercrimes affecting a person's property have arisen. Cyber vandalism to steal information from other organizations or to steal someone's bank data, using software to gain access to an organization's website, and so on are examples of these forms of cybercrimes. This is equivalent to when a criminal unlawfully obtains a person's bank or credit card information. In cybercrime, a hacker steals a person's bank account information to gain access to money, makes online transactions or runs phishing schemes to trick people into giving away their personal information. They may also use some malicious software to gain access to a web page containing sensitive data. Computer vandalism, intellectual property crimes (Copyright, proprietary, trademark, etc.), online threatening, and so on are examples of these types of crimes. The following are examples of cybercrime against property:

    - Computer thievery.
    - Virus transmission.
    - Trespassing on the internet.
    - Unauthorized control or connection to a computer system.
    - Thefts on the internet.
    - Software piracy is an example of an intellectual property crime.
    - Infringement on a copyright.
    - Infringement on a trademark.

iii. Governments or organizations are the targets of criminal activity

Certain cybercrimes have been perpetrated to pose a danger to foreign governments or organizations. These cybercrimes are primarily carried out to instill fear among the citizens of a specific country. Governments of hostile countries, militant organizations, belligerents, and others can be the instigators or perpetrators of such crimes. Cybercrime against the government can take the form of a cyber-attack on a government website, a cyber-attack on a military website, or cyber terrorism, among other things. Cybercriminals hack government or agency websites, government firms, and military websites to spread propaganda, intimidation, or rumors in this type of cybercrime. Cybercrimes against governments or organizations are the name given to these types of cybercrimes. The few examples of government or organization-related crime are as follows:

- Unauthorized access to a computer system and control of it.
- Terrorism against the government or an institution by the use of the internet.
- Unauthorized documents in one's possession.
- Piracy software is distributed.

iv. Cybercrime Against Society

It refers to cybercrime that has a broad impact on society. These illegal activities are carried out with the intent of causing damage or altering cyberspace so that a large number of people are affected. The general population and social interests are the primary targets of these forms of crimes. The following forms of cybercrime against society are included:

- Pornography involving children.
- Indecent disclosure of financial crimes committed by polluting children.
- Unauthorized merchandise sales
- Human trafficking
- Fraud.
- Internet gambling.
- Web jacking is a term used to describe the act of stealing a website.

CYBER SECURITY BREACH

Cyber protection is a method used to prevent unauthorized access to computers, networks, services, personal data, etc. It is an operation that protects and defends information and other communication systems from the unauthorized use, alteration, or misuse of the computer. Cybersecurity is often referred to as security of information technology. It covers device, networks, software, and data protection strategies for unauthorized access or assaults, which can harm them in some way or use them. Cyber-security is essentially a technological solution for safe networks.

Concept of Cyber Security Infringements

Cybersecurity infringements lead to unauthorized or unauthorized access to computer systems, networks, storage data, software/equipment, facilities, and devices by violating system security mechanisms. Infringements of cybersecurity occur when security policies, mechanisms, or systems are breached.

Simply put, if a person (read cybercriminal) enters a private or sensitive area in the IT illegally, there is a cybersecurity violation. A violation of cyber safety is also recognized as a violation of cybersecurity. One of the early phases of a cyber-assault by a malicious intrusion such as a hacker, cracker, or program is a cybersecurity violation. Depending on the nature of the incident, cybersecurity breaches can vary from low risk to highly critical.

Security violations are closely monitored, detected, and processed in an entity or enterprise through a software or hardware firewall. This firewall gives your network or security administrator a warning if any intrusion, infringement, or violation is detected.

When an unauthorized party enters security measures to gain access to secure areas of a system to gain information or spread viruses, this is referred to as a cybersecurity breach. A cybersecurity breach can give hackers access to sensitive information such as company accounts, intellectual property, and consumer personal information. A security breach occurs when a cyber attacker steals such sensitive information. This type of knowledge is often sold on the dark web and can be used to commit crimes like identity theft.

Cyber Security Importance

Good cyber protection is extremely critical for an enterprise to avoid its data and infrastructure being violated and misused. Cyber-attacks are costing organizations, which may cause

collateral harm, billions of pounds. Critical data and fines and reputational harm are to be lost to impacted organizations. Security of cyberspace is critical because

- There are increasing costs of cyber breaches: A robust cybersecurity system is considered to avoid data breaches of the customer as an organization's obligation. As privacy laws emerge and become commonplace, organizations are increasingly responsible for this. If security violations occur, the institutions will be severely fined. Non-financial costs like reputational harm often have to be taken into account.
- Cyber-attacks continue to develop: cyber-attacks continue to increase in complexity as science and technology develop, and cyber-attackers break into someone's system through high-tech technologies. Social engineering, malware, and ransomware are among them (used for Petya, WannaCry[10] and NotPetya[11]).
- Cybercrime is an important financial gain industry. The cybercrime industry was valued at $1,5 trillion, according to a Bromium survey in 2018. But money is not the only factor; attackers may also be influenced by politics, ethics, or social motives.
- Cyber protection is a key problem for the board: New legislation and reporting standards make surveillance of cybersecurity risk[12] a challenge. The board will continue to provide management with guarantees that its cyber-risk policies will reduce the risk of attacks and limit its financial and operational impacts.

Effect of a cyber security violation

A successful infringement of cyber security will cause a company and its business serious harm. It can affect the standing and customer confidence of companies. The impact of an infringement differs for each company according to time and time, type of infringement and industry. For instance, an infringement of data may be more important for the finance industry than the manufacturing sector. However, the cyber security violation has some common impacts. The effects of an infringement of cyber safety can be split into five categories:

- Cybercrime is unreasonably more expensive than large companies. **financial losses**: The financial effect can hit millions for a large company, but these monetary consequences hardly affect them. Small companies on the other hand are shelling Rs. 26,85,859 on average to recover direct costs alone from one single data breach. An

[10] https://blog.itgovernance.co.uk/blog/wannacry-ransomware.
[11] https://blog.itgovernance.eu/
[12] https://www.itgovernance.co.uk/cyber-security-risk-management

agency or a company can be put out of business by careless incompetence on cyber security. Companies who have experienced a cyberattack usually often incur costs related to the repair of systems, networks and equipment affected. Cyberattacks often result in significant financial losses as a result of:

- Traders are being disrupted (e.g., inability to carry out transactions online).
- Loss of a company or deal.
- Theft of money or financial records.

❖ **Reputable Harm:** cyberattacks can damage a company's credibility and corrode customers' confidence in this company. The effect of reputational harm can also affect suppliers or affect connections with shareholders, investors, and other third parties.
Loss of consumer and stakeholder confidence can be one of the most damaging effects of a cyber security violation. Most people would not wish to do business with an entity or company broken and attacked by a weak cyber safety system, especially if the customer data were not protected. The reputational success will also impact the company's ability to employ the best talent, suppliers, investors and consumers. This may lead, in turn, to:

- Customer loss.
- Sales loss
- Profit reduction.

❖ **Theft**: Smaller businesses' protections and protection mechanisms are much less sophisticated and easier to breach than larger businesses', making them a softer target. Money is lost in cyber frauds and robberies, but stolen data is worth more to hackers, particularly when sold on the Dark Web. For example- on 31 October 2019, it was found that about 1,3 million debit and credit card data were sold by hackers on the Dark Web, that each card was sold to 100 dollars and that overall hackers were able to make $130 million. Theft of intellectual property is equally harmful; businesses may lose several years of effort and investment in research and development of trade secrets or content protected by copyright. Theft[13] can take many forms, such as:

- Theft of confidential information from a business.

[13] https://www.lexology.com/

- Theft of financial data (such as bank account numbers or credit/debit card numbers).
- Customers' personal information is stolen.
- Theft of money is a serious crime.
- Theft of one's identity.

CASE

Yahoo! Inc[14] v. Akash Arora & Anr: In this case, the defendant created a virtually identical website to the plaintiff's well-known website and offered similar services. The court ruled in favour of Yahoo Inc. (the Plaintiff trademark)'s rights and against the defendant, which had registered itself as YahooIndia.com. "It was an attempt to profit from the popularity of Yahoo's trademark," the Court said. A domain name registrant does not acquire the legal right to use the specific domain name simply by registering it; he can also be liable for trademark infringement.

Government of India's Cybersecurity Initiatives

Over the last few years, the number of cyber security incidents in India has steadily risen. Mr. PP Chaudhary, India's Minister of State for Electronics and IT, reported that 44,679, 49,455, and 50,362 cyber security incidents occurred in India in 2014, 2015, and 2016, respectively, according to data collected CERT[15]. Phishing, website intrusions and defacements, virus and denial-of-service attacks are only a few of the events that have occurred. According[16] to the '2016 Cost of Data Breach Study: India,' the average overall cost of a data breach charged by Indian businesses increased by 9.5 percent. In comparison, the per capita cost increased by 8.7 percent and the average size of a breach increased by 8.1 percent. Although the government[17] has taken some cyber security steps, more expansive and ambitious measures are needed to meet the rising challenges as discussed below.

- **National Cybersecurity Policy, 2013**

  National Cyber Security Policy, 2013: the Indian Government took an initial official move towards cyber-security in 2013, as described in the National Cyber-Security Policy of 2013, Department[18] of Electronics and Information Technology. The policy

[14] https://indiancaselaws.wordpress.com/2015/07/15/yahoo-inc-v-akash-arora-anr/
[15] India's Computer Emergency Response Team
[16] http://tech.firstpost.com/news-analysis/
[17] https://securityintelligence.com/
[18] https://www.meity.gov.in/

aims to create a safe and resilient cyber area for individuals, companies, and the government. It has the task of protecting information and infrastructure for cyberspace, building capacity to avoid and respond to cyber-attacks, and minimizing harm through coordination of institutional systems, personnel, processes, and technology efforts.
The policy's objectives include developing a secure cyber ecosystem, adhering to global security standards, strengthening the regulatory framework, establishing round-the-clock mechanisms for gathering intelligence and effective response, operating a National Critical Information Infrastructure Protection Centre to protect critical information infrastructure 24 hours a day, seven days a week, and conducting research and development.

Creating a stable cyber environment through initiatives such as a national nodal agency, encouraging organizations to appoint a member of senior management as the Chief Information Security Officer, and developing information security policies are among the strategies embraced by this Policy.

- Creating a mechanism for assurance.
- Encouraging the adoption of open standards.
- Strengthening the regulatory system by periodic reviews, harmonization with international standards, and increased public understanding of the legal framework are all priorities.
- Creation by national frameworks and processes of mechanisms to address security threats and responses. Emergency Response Team National Computer[19]
- Functions as the core department for co-ordination, emergency response and crisis management in all cyber security efforts.
- Ensuring e-governance through the implementation of best global practices and broader use of key public infrastructure.
- The National[20] Critical Information Centre operates as a nodal entity to protect and resilience critical information facilities.
- Encouraging state-of-the-art data security infrastructure research and development.
- Development of human resources by training and capacity building programmes.

[19] www.cert-in.org.in/ (CERT-in)
[20] https://www.nciipc.gov.in/

In 2014, the Office of the Prime Minister set up the role of National Coordinator on cyber security. The Ministry of Electronics and Information[21] Technology released numerous orders and guidelines in 2016 to intrude by the notorious 'Legion' hacker community. These included using NPCI[22] for financial sector audits, IT review and strengthening, Twitter social networking website guidelines to reinforce its network, and guidelines to all financial stakeholders including digital payment companies to report unusual incidents immediately. The National Technical Research Organisation, the National Intelligence Grid, and the National Information Board are some Indian organisations that deal with cyber security. To improve cybersecurity in India, India's first chief information security officer[23] was appointed in 2016, and all ministries were then required to nominate Central Information Security[24] Officers. The government of India has recently implemented some additional important steps to resolve cybersecurity concerns, as discussed below.

Cyber Swachhta Kendra' (Botnet Cleaning and Malware Analysis Centre)

In February 2017, the Government of India's Center for Emergency Response (CERT-in) unveiled a new desktop and mobile protection solution for Internet security in India, entitled 'Cyber Swachhta Kendra' (Botnet Cleaning and Malware Analysis Centre).

This center operates by CERT-in according to Section 70B of the IT Act of 2000. The solution is part of the Digital India initiative of the Ministry of Electronics and Information Technology to detect botnet infections in India and prevent further infections by notifying end-user systems, enabling their own to be cleaned and secured. It works to analyze the BOTs, supply information, and allow citizens to remove BOTs and malware and make people aware that data, computers, mobile phone systems, and devices such as home routers should be protected. The Cyber Swachhta[25] Kendra is a step towards India's development of a stable cyber environment as provided for by the Indian Cyber Security Policy. This center cooperates closely with ISP[26]s and product/virus companies in notifying end-users of device infections and providing help to clean the systems and industry and academia to detect bot-infected systems. The center seeks

[21] https://www.meity.gov.in/
[22] Indian National Payment Company
[23] https://www.mod.gov.in/ (CISO)
[24] http://economictimes.indiatimes.com/
[25] https://www.cyberswachhtakendra.gov.in/
[26] Internet Service Providers

to make popular users aware of a botnet, malware infection, and steps to protect their computers, systems, and devices against malware infection.

The following security and protection tools are available from the government:

- The government also launched “USB Pratirodh,” a program aimed at preventing unauthorized use of removable USB storage media devices such as pen drives, external hard drives, and USB-supported mass storage devices to Union IT and Electronics Minister Ravi Shankar Prasad.
- There was also a new app called "Samvid." It's a Windows application whitelisting solution that runs on the desktop. It only allows a pre-approved collection of executable files to run and prevents suspicious programs from running on the desktop.
- M-Kavach[27], an Android mobile device protection device, has also been developed. It protects against malware that steals personal data and passwords, misuses Wi-Fi and Bluetooth services, is lost or stolen, sends spam SMSs, premium-rate SMS, and receives unwanted/unsolicited incoming calls.
- Browser JSGuard is a browser extension that detects and defends malicious HTML & JavaScript attacks made via the web browser using Heuristics. It warns the user when he visits malicious web pages and offers a comprehensive analysis threat report.

RISE IN CYBERCRIMES IN PANDEMIC LOCKDOWN

‘During this precarious lockdown, working from home (WFH) has become the standard. The methods for completing tasks have changed dramatically, with working from home now being the only viable alternative. After the COVID-19 pandemic-imposed restrictions on physical gesticulation, people's reliance on the internet has grown exponentially. Video conferencing, seminars, online lectures, and chatting have also increased online traffic. The use of Paytm, Google Pay, BHIM, Phonepe, and others to make payments has also increased.

Along with changing working practices, the modus operandi of criminals has also changed during the lockdown. While crime has decreased as a result of people staying at home, online fraud has increased. Apart from serving as interaction/communication interfaces, they may also serve as forums for criminal elements, leading to the emergence of significant security issues.

[27] http://tech.firstpost.com/news-analysis/

Working from home has now become an avenue for cybercriminals to take advantage of people by e-mail scams, password cracking, phishing, extortion attacks, and online sexual abuse, among other things.

Cybercrime instances during a pandemic

- According to the Maharashtra Police Cyber Security Crime Wing, fraudulent ties to COVID-19 circulate through social networks and Whatsapp.
- The fear and vulnerability of the people to the coronavirus are manipulated through these fraudulent communications.
- According to the officials, these messages are distributed: Promising jobs to people between the ages of 18 and 40, with a Class certificate and a monthly wage of Rs. 3,500 during the lockout, Remedies and extra protection for Coronavirus, Free recharge of Netflix or other video streaming services, Free internet data, and Sale of liquor deals.
- These texts, however, have malicious connections. These links were developed to collect information, including confidential and personal information stored on the user's devices.
- The ties contribute to different attacks and malware and thus jeopardize the system and the internal data security. Since the lock-in makes them vulnerable to such attacks, people's online presence has increased.

Role of Media

Indeed, it is a question that will most probably often receive a negative answer. No, the use of social media does not inherently increase the protection of the company's system because an employee can quickly provide information on social media platforms that is not necessarily confidential and a potential key to opening backend security loopholes. Besides, a post can be deleted from your Facebook or Instagram account, but when it is in cyberspace, the sender's mobile device cannot just destroy it. It must be destructed or deleted with the main server, which can only be accessed by a few who manage the entire cyber-space hierarchy. But reverse psychology has made it possible for digital users to become indirectly conscious of the need not to reveal individual details on an open forum. Even though the shared personal information is not sensitive, it may still be a potential target for a cyberattack.

Reforms in the law are required

The Information and Technology Act of 2000 establishes a system for electronic governance protection by allowing electronic documents and digital signatures to be identified. It also spells out the consequences for cybercriminals. It has enacted legislation to establish a Cyber Appellate Tribunal to settle conflicts involving cybercrime and online fraud. Additionally, depending on the circumstances and the Court's discretionary powers, some of the statutory provisions of the Indian Penal Code, 1860 in the crimes of Fraud, Criminal Intimidation, Cheating, Breach of Trust, Abetment of Suicide by Blackmailing, and others may be charged against an accused. However, an individual cannot be punished twice for the same offense because this would violate his Fundamental Right to Due Process guaranteed by Article 20[28] (2) of the Indian Constitution.

CONCLUSION

When cybercrime is on the rise, and when Internet users are growing, there is a need for a user-friendly law that protects internet users and makes the internet users reliable. After examining all forms of cybercrimes and legal pronouncements, it can be seen that the violation of Internet users' rights is poorly implemented and deliberately ignored. There is no fixed provision that can be enforced in cyberspace, if the user's rights are breached, but a mixture of different provisions and legislation which can put them under one umbrella. The consumer protection act and the IT Act must be amended to make cyber crimes a violation of internet users' rights. A strong international cybersecurity regime is urgently needed to address all needs of various concerns and questions. By applying governance, management, and inclusiveness principles,it is possible to establish, enforce and promote a common approach to cybersecurity. This encourages a cybersecurity infrastructure that eventually leads to an instinct about what is secure and risky.

Need to create an international multi-stakeholder regime including business, government, international, and non-governmental cybersecurity organizations. Besides this, cyber law has also emerged globally, fostering the development of modern law and cyber law aspects.

[28] Double Jeopardy.

REFERENCES

- https://www.lexology.com
- https://blog.ipleaders.in/
- https://www.cyberswachhtakendra.gov.in/
- https://www.cert-in.org.in/
- https://blog.ipleaders.in/cyber-security-law/
- https://www.lexology.com