EDUZONE: International Peer Reviewed/Refereed Multidisciplinary Journal (EIPRMJ), ISSN: 2319-5045
Volume 11, Issue 2, July-December, 2022, Impact Factor: 7.687 Available online at: www.eduzonejournal.com

Cyber Security Issues in India

Mr. Pankaj[1], Ms. Shalu Kumari[2], Ms. Shikha Sharma[3]

[1,2,3]MBA Student, Ganga Institute of Technology and Management, Kablana, Jhajjar, India

ABSTRACT

Over the past year, India has experienced a number of noteworthy and unusual occurrences that have elevated the importance of cyber security for the country's banking industry to a level never seen before. The Government of India's current endeavor, known as the flagship Digital India programme has been the most significant contributor in this regard. The programme aims to convert India into a knowledge economy and society that is enabled by technology. The abrupt increase in digital transaction value and volume, which reached all-time highs in March 2017, is evidence of the faster transition to electronic payments. With the total number of accounts surpassing 29.18 crore the Pradhan Mantri Jan Dhan Yojana (PMJDY) has contributed to the ongoing expansion in inclusive banking penetration, bringing new and uninitiated customers into the fold of financial services. Incidents and risk concerns also became apparent. The penetration of a major bank's SWIFT payment application and the ensuing large-value fraudulent fund transfer were two of the significant occurrences. Another was the widespread compromise of numerous banks' debit cards through a sophisticated and persistent attack on a payment processor.

INTRODUCTION

The Greek term kubernētēs, which means pilot or steersman, is where the word "cyber" first appeared in the field of cybernetics.In actuality, American mathematician Norbert Wiener popularized it. In the 1940s, he wrote a book titled Cybernetics. This was his forecast for a world where autonomous PCs rule everything. framework that would develop further and have its own feedback loop. Actually, the term "cyber" didn't start to be associated with other phrases that indicated anything to do with digital until the 1980s. Cyberspace is "associated with or typified by computers, virtual reality, or information technology. When we say that we live in the "cyber age," we're referring to the information technology, virtual reality, and analyst era. The cyber universe is growing, just like the actual cosmos.

When hackers attempt to compromise or harm a computer system or network, it's called a cyber attack. The imaginary space where computer network communication takes place is known as "cyber space." The phrase first appeared in popular culture in science fiction. However, a lot of individuals utilize it now, including corporate leaders, security experts, and technological strategists in addition to the military. Cyberspace is the term we use to characterize the domain of the global technological environment. Man is now completely dependent on the Internet for all of his requirements due to technological advancements, which has an impact on both the individual and the larger society. It has made it possible for man to easily access everything while seated in one place. Everything a person could possibly want—social networking, online shopping, data storage, gaming, online education, and online employment opportunities—is possible with the aid of the Internet. It is consumed and used in every manner imaginable. With the growth of the internet and all of its benefits came the concept of cybercrimes. The founding fathers had no clue at all when the Internet was initially developed that it could be abused by criminal activity. A few years ago, people were unaware of the infractions that could be done via the internet. When invention grows, so does the misuse of it.

has expanded to the perfect extent. The amount of cybercrime has skyrocketed from the year 2000. Cybercrimes can endanger the financial stability of an organization, the security of a nation, or even a single person. India is Comparably not far behind other countries where the frequency of digital infractions is rising daily.

Cyber Crime:

Any malefactor or other offense involving electronic communications, information systems, the web, or any combination of these can be classified as "Cyber Crime" .Cybercrime is any crime that involves a network and a framework, or system. The computer could have been the object or goal of the crime, or it could have been used in its commission. Digital crimes are actions committed with the intent to hurt a person or people, primarily through the use of contemporary telecommunications, with the goal of intentionally harming the victim's reputation or causing them physical or psychological distress. For instance, notice feeds, emails, texts, cell phones, and Web chat rooms. The security and economic stability of the nation are threatened by these kinds of crimes. These kinds of crimes are among the most well-

known issues, particularly those involving copyright violations, hacking, and child pornography. When confidential information is suppressed or made public, whether through legal means or not, there are further security risks. Cybercrime incidences have increased astronomically as a result of the massive rise in online share trading and electronic commerce (e-commerce).

Cyber Crimes can be mainly divided into 3 major classifications:

- Cyber Crimes against persons
- Cyber Crimes against property
- Cyber Crimes against government

Cybercrimes against Persons:

Cybercrimes against people encompass a range of acts, including the dissemination of child pornography and the harassment of individuals via computer-related activities like email. Trading, sharing, uploading, and dispersing pornographic and indecent public nudity content is one of the most significant forms of cybercrime that exists today. These crimes do not cause much harm to humanity. This cybercrime poses a threat to the next generation's development because, if left unchecked, it will leave the younger generation with permanent wounds and scars. A distinct kind of cybercrime is cyber harassment. Harassment in the many forms can and does happen in cyberspace or when using cyberspace. Harassment might be ethnic, religious, sexual, or other types. Individuals who engage in this kind of harassment are also breaking the law online. Cyber bullying has the potential to spread crime to other connected areas where citizens' privacy is violated. Cybercrime that involves violating the privacy of internet users is very severe. Nobody enjoys having their most sensitive and priceless privacy—which citizens have access to over the Internet—attacked by others.

Cybercrimes against Property:

Cybercrimes against any kind of property are the second category of cyber attacks. Computer vandalism, or the destruction of another person's property, is one type of crime. Other crimes include sending harmful programs, stealing money from financial institutions, and stealing confidential data and information. A start-up company in Mumbai suffered significant financial losses after a corporate cyber spy helped the rival organization, a prominent player in the industry, steal the technical database from their PCs.

Cybercrimes against Government:

The growth of the internet has shown that individuals and organizations are using cyberspace as a means of posing a danger to both national and international governments as well as to its citizens. When someone "crashes" into a website run by the government, the military, or another entity, this crime turns into terrorism.

Cyber Crime in India

India is ranked third globally among the top 20 countries where cybercrimes occur, according to the United States Internet Crime Complaint Centre (IC3) of the Federal Bureau of Investigation's 2019 Internet Crime Report. The United Kingdom led the list, with 93,796 victims of cybercrimes, followed by Canada (3,721) and India (2,901), the report states, excluding the United States.
The latest data from the National Crime Records Bureau (NCRB) shows that 27,248 incidents of cyber attack were reported in India in 2018. At about the same time, 1,205 cyber attack incidences were registered in Telangana. Since its launch a year ago, the Central government's National Cyber Crime Reporting Portal has received 33,152 complaints, resulting in the filing of 790 FIRs. The IT Act does not exclusively address cybercrime. The Indian Penal Code also has several sections.

Following are the few examples of Cybercrime in India:

E-Mail Bomb: An example of an Internet abuse is a "e-mail bomb," which is when a specific email address is bombarded with a high number of emails with the intention of overloading the mail server, crashing the service, and flooding the inbox.

Hacking: Hacking is the attempt to abuse a private network or a PC framework. In essence, it refers to unauthorized access to or control over PC security frameworks for illicit purposes. Hackers with advanced skills in breaching security systems carry it out.

Spreading computer viruses: A PC infection is a hostile application that is loaded onto a client's PC without the client's knowledge and engages in destructive operations, such as erasing data. It can proliferate via email, the web, multimedia, and pen drives (secondary storage).

Phishing: It is a type of cybercrime in which a person poses as a legitimate business and sends emails, phone calls, or instant messages to one or more targets in an attempt to trick them into divulging sensitive information such as passwords, credit card numbers, banking information, and identifiable information. This information is then utilized to access important records, which may result in widespread fraud, identity theft, and financial loss.

Identity theft: The act of obtaining someone else's personal or financial information with the sole intent of using that person's name or identity for transactions or purchases is known as identity theft. It entails gaining access to business databases in order to purloin client lists and destroy credit and private information. The offender faces the possibility of serving three years in prison of any kind in addition to a fine of up to one lakh rupees as punishment.

Cyber Security:
Hackers breach a hospital's patient data, make derogatory remarks about a political figure on social media, and compromise the power grid. Despite their apparent differences, all of these scenarios may fall under the category of cyber security. Businesses and the government in particular often define cyber security. Cyber security is the definition of methods and procedures used to safeguard data. It is relevant to digital data. Data on a server, network, or system that is being used, saved, or communicated .The lifeblood of cyberspace is information. Massive amounts of data, from personal to high-level state communication, are transferred across networks and stored on devices and data centers. It would be impossible to discuss cyber security without bringing up technology.

"Cyber-security" is defined under the IT Act, 2000 as the protection provided to devices and data stored on them against "unauthorized access, use, disclosure, disruption, modification or destruction."

Governmental organizations and cyber security regulations:

1. The primary organization tasked with safeguarding the nation's vital infrastructure and managing cyber security events in key industries is the National Technical Research Organization.
2. The responsibility for responses, such as analysis, projections, and alerts regarding cyber security breaches and issues, rests with the Indian Computer Emergency Response Team.

Techniques for Cyber security

1. Strong Password Security: The simplest way to increase system security is to use a complex and strong password. For instance, a password that consists of letters, numbers, and special characters. Updating it frequently can assist in preventing brute force password cracking.
2. Knowledge authentication: Update frequently and use caution when using: Use caution when using email and the internet as hackers and programmers can misuse them in many ways.A system update and regular backup program are fantastic ways to ensure that your data can be retrieved, as well as to safeguard and fix any errors or flaws in the system.
3. Malware scanners: Programs that check all files on the device for dangerous viruses and malicious code. Malicious software samples that are frequently grouped together and referred to as viruses, worms, and Trojan horses are called malware.
4. Firewalls: A piece of hardware or software that assists in sifting out viruses, worms, and hackers who try to infect your device through the internet. Every message entering or leaving the internet is screened by the firewall, which checks each one for compliance with safety regulations and bans any that don't.
5. Anti-virus software - Installing anti-virus software is essential to preventing viruses from infecting your computer network. It aggressively checks your system documents and emails for viruses that could infect your operating system. A decent antivirus program should be compatible with the system and update on a regular basis.

Cyber ethics and countermeasures against cyber attacks:

It alludes to the online code of conduct for responsible behavior. The basic rule is to attempt to avoid doing anything online that you would view as improper or unlawful.

1. Use the internet to communicate and share with others. Keeping in touch with friends, family, and coworkers is made easier with email and texting. distributing fresh ideas, ideas, and knowledge to people in the neighborhood or worldwide.
2. Never communicate or share personal information, such as your password, bank account number, ATM pin, or other details, via an unencrypted network, including unencrypted mail. The decoded websites are those that lack the lock icon and https in the browser's address bar. The letter "s," which stands for "secure," indicates that the website is safe and secure.
3. Wait till a social networking site or platform is genuine and legitimate before signing up.
4. Always remember to upgrade and refresh the operating system. On one's computer, software such as firewalls, antivirus, and anti-spyware programs should be installed and updated often.
5. Don't browse, follow, or reply to unscrupulous websites or links.
6. Avoid using the Internet to harass or intimidate anyone. Avoid using derogatory words or phrases. It is improper to disparage someone, email offensive or embarrassing images of them, call them names, or try to harm them.
7. The Internet is regarded as the world's largest library, containing knowledge on every topic in any field of study. Thus, make appropriate and lawful use of this data.
8. Never give out your password to third parties and never use someone else's password to access another person's account.
9. Never give out your personal information to anyone because there's a good chance someone else may misuse it and you'll be held accountable.
10. Avoid clicking on pop-ups on e-commerce websites or any other website that offer site surveys or studies, as they may contain harmful software. Drive-by-download is the term for the background download that happens when we accept or click on pop-ups. This file contains malware and malicious code.
11. Never lose copyrighted information, and only download games or videos that are permitted.
12. Never try to infect another person's computer with malware of any kind.
13. Refrain from using false identities and creating accounts under false pretenses, since this could put both you and the other person in danger.

These are a few Cyber Morals that one should abide by when using the internet. From a very young age, we adopt suitable values and behaviors in our life, and the same is true in the cyber realm.

CONCLUSION

India, a nation of 1.3 billion people, has the cheapest data plans worldwide. With the advancement of networks, data and information security is becoming increasingly crucial. This study makes it very evident that as technology and cyberspace advance, so will the range of cyber threats. To protect data, one must implement cyber security measures such as firewalls, strong passwords, antivirus software, and cyber attack prevention techniques. India has to switch from a reactive to a proactive strategy to cyber system protection. Currently, the country only protects cyber systems when cyber security incidents arise. since it is now necessary. To preserve the rule of law, protection of rights and privacy requires awareness, firm modifications, penal provisions, and cyber security policies. These are all necessary.

REFERENCES

[1]. https://alpinesecurity.com/blog(Visited on 18th April, 2020)
[2]. https://www.cisomag.com/india-cybersecurity-policy/(Visited on 21st April, 2020)
[3]. Sumanjit Das and Tapaswini Nayak, “IMPACT OF CYBER CRIME: ISSUES AND CHALLENGES” 6 IJESET 142-153 (2013).
[4]. https://cybercrime.org.za/definition(Visited on 24th April, 2020)
[5]. https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (Visited on 25th April, 2020)
[6]. https://delhidistrictcourts.nic.in/ejournals/CYBER%20LAW.pdf(Visited on 27th April, 2020)
[7]. https://www.cyberralegalservices.com/detail-casestudies.php(Visited on 2nd May, 2020)
[8]. http://www.helplinelaw.com/employment-criminal-and-labour/CDII/cyber-defamation-in-india.html (Visited on 6th May, 2020)
[9]. Puja Gupta and Rakesh Kumar, “Security Risk Management with Networked Information System: A Review”4 (2) IJEE193– 197 (2012).
[10]. Veenoo Upadhyay, Dr. Suryakant Yadav, “Study of Cyber Security Challenges Its Emerging Trends: Current Technologies”5 IJERM 2349-2058 (2018)