Cyber Jaagrookta Diwas(Sep.2022)

Unit 1: Cyber Crimes and Safety

The crime that involves and uses computer devices and Internet, is known as cybercrime.

Cybercrime can be committed against an individual or a group; it can also be committed against government and private organizations. It may be intended to harm someone's reputation, physical harm, or even mental harm.

Cybercrime can cause direct harm or indirect harm to whoever the victim is.

However, the largest threat of cybercrime is on the financial security of an individual as well as the government.

Cybercrime causes loss of billions of USD every year.

Types of Cybercrime

Let us now discuss the major types of cybercrime −

Hacking

It is an illegal practice by which a hacker breaches the computer's security system of someone for personal interest.

Unwarranted mass-surveillance

Mass surveillance means surveillance of a substantial fraction of a group of people by the authority especially for the security purpose, but if someone does it for personal interest, it is considered as cybercrime.

Child pornography

It is one of the most heinous crimes that is brazenly practiced across the world. Children are sexually abused and videos are being made and uploaded on the Internet.

Child grooming

It is the practice of establishing an emotional connection with a child especially for the purpose of child-trafficking and child prostitution.

Copyright infringement

If someone infringes someone's protected copyright without permission and publishes that with his own name, is known as copyright infringement.

Money laundering

Illegal possession of money by an individual or an organization is known as money laundering. It typically involves transfers of money through foreign banks and/or legitimate business. In other words, it is the practice of transforming illegitimately earned money into the legitimate financial system.

Cyber-extortion

When a hacker hacks someone's email server, or computer system and demands money to reinstate the system, it is known as cyber-extortion.

Cyber-terrorism

Normally, when someone hacks government's security system or intimidates government or such a big organization to advance his political or social objectives by invading the security system through computer networks, it is known as cyber-terrorism.

Cyber Security

Cyber security is a potential activity by which information and other communication systems are protected from and/or defended against the unauthorized use or modification or exploitation or even theft.

Likewise, cyber security is a well-designed technique to protect computers, networks, different programs, personal data, etc., from unauthorized access.

All sorts of data whether it is government, corporate, or personal need high security; however, some of the data, which belongs to the government defense system, banks, defense research and development organization, etc. are highly confidential and even small amount of negligence to these data may cause great damage to the whole nation. Therefore, such data need security at a very high level.

1. **Inappropriate and unsuitable content for children**

   Children out of their own curiosity, under peer pressure or during their search accidentally might come across content which is not suitable for viewing at their age. Viewing inappropriate content (such as sexual or pornographic material, incidences of abuse and violence, content propagating radical/extremist ideologies etc.) may leave an impact on their young impressionable minds. Parental guidance is thus necessary to safeguard children from being exposed to such explicit content online. Child-friendly web-browsers could be installed to block such inappropriate content and websites so that children do not access information which may scar them for life.

2. **Cyber-predators and cyber-bullying**

   Predators, who exploit vulnerabilities of young children often access social networking websites and spaces for chats and social interactions to exploit children. They often capitalize upon the element of anonymity to befriend children and subject them to high risks to their safety and security such as abuse or violence. Cyber-bullying through social media platforms have also become a prevalent peril. It is thus critical for parents to encourage children to trust them and confide in them about their social interactions online, especially about those that cause distress to them. Children should also be educated to call CHILDLINE 1098 in case they want to report or talk about cyber bullying.

3. **Online scams**

   - Children are also vulnerable to 'Online Scams' which are often targeted at adults for coaxing money out. Several scams and false schemes such as encouraging claims to lottery winnings, requesting payments to receive awards, gifts and winnings, websites offering products at cheap prices etc. lure children into accessing these schemes. In most cases, children either end up sharing parents' or guardians' financial information or lead to entrapping their families into bigger scams and ponzi schemes. It is important to make children aware of such scams and educate them on the implications that such schemes might have in future.
   - CHILDLINE 1098 is available 24x7 for children in distress. CHILDLINE provides a listening ear to children who wish to talk about/report cyber-threats and seek guidance to pacify the problem.

In the last few years, cybercrime, such as phishing, identity theft, and fraud, has skyrocketed. In the last year itself, India recorded a 16% jump in the number of cyberattacks across the country. Cybercrime penetration is likely to continue to intensify. This stresses the importance of developing more effective and deterrent legal frameworks as well as more strict cyber crime laws in India. In the given scenario, it becomes interesting and even necessary to follow the existing cyber crime laws in India and analyze whether they provide enough coverage against these crimes or not. So, let's take a detailed look at the existing cyber law in India and what developments and improvements we can expect in the future. Increase in Cyber Attacks on Systems Cybercrimes are currently ruling major newspaper headlines globally - causing unanticipated damages across industries and individuals. The predominant forms of cyber thefts include - data breaches, identity theft, financial theft, and internet time thefts, amongst others. Though cybersecurity & cyber laws are advancing

every day, hackers are also constantly upping their game and finding ways to break into new systems. This reinforces the need not only for better cybersecurity systems but robust cyber laws in India as well along wit other countries. Further, to mitigate the cyber crimes and curb the efforts of the fraudsters, cyber crime law makers need to be abreast of the potential loopholes in the cybersecurity landscape and fix them in real-time. Persistent efforts with constant vigil are crucial to controlling the escalating risks nationwide. Why Cyber Crime Laws in India? Every government in the world, including our own country, is concerned about cyber security. India is especially facing a rising number of cyber security issues, and it is critical that it accepts the responsibility for them. According to a recent Economic Times analysis on global cybercrime, cyber-attacks cost the government nearly Rs. 1.25 lakh crore every year. Another research by Kaspersky highlights that the number of cyberattacks in India increased from 1.3 million to 3.3 million during the first quarter of 2020. India recorded the largest number of attacks, 4.5 million, in July 2020. Recently, the Reserve Bank of India (RBI) prohibited MasterCard from failing to comply with the direction for storing payment system data. The hazards posed by the internet are nearly limitless, and the most effective method to resist them is to implement a cyber security policy. The government must devote significant resources to safeguarding key data assets. The country's cyber security law has to be updated to integrate legal rules and address the issues posed by rapidly developing technologies.

Types of cyber crime act in India?

There are four predominant cyber laws to cover when it comes to cyber security: In countries like India, where the internet is used very extensively, cyber laws in India become extremely crucial. Stringent cyber laws fulfill the purpose of supervising the digital circulation of information, software, information security, e-commerce, and monetary transactions. By providing maximum connectivity and minimizing cyber security concerns, India's Cyber security Law has cleared the path for electronic commerce and electronic government in the country and also broadened the scope and application of digital media.

1. **Information Technology Act, 2000**

   The Indian cyber law is governed by the Information Technology Act, penned down back in 2000. The principal impetus of this Act is to offer reliable legal inclusiveness to e-Commerce, facilitating registration of real-time records with the Government. But with the cyber attackers getting sneakier, topped by the human tendency to misuse technology, a series of amendments followed. The ITA, enacted by the Parliament of India, highlights the grievous punishments and penalties safeguarding the e-governance, e-banking, and e-commerce sectors. Now, the scope of ITA has been enhanced to encompass all the latest communication devices.

   The IT Act is the salient one, guiding the entire Indian legislation to govern cybercrimes rigorously:

   Section 43 - Applicable to people who damage the computer systems without permission from the owner. The owner can fully claim compensation for the entire damage in such cases.

   Section 66 - Applicable in case a person is found to dishonestly or fraudulently commit any act referred to in section 43. The imprisonment term in such instances can mount up to three years or a fine of up to Rs. 5 lakh.

   Section 66B - Incorporates the punishments for fraudulently receiving stolen communication devices or computers, which confirms a probable three years imprisonment. This term can also be topped by a Rs. 1 lakh fine, depending upon the severity.

   Section 66C - This section scrutinizes the identity thefts related to imposter digital signatures, hacking passwords, or other distinctive identification features. If proven guilty, imprisonment of three years might also be backed by a Rs.1 lakh fine.

   Section 66 D - This section was inserted on-demand, focusing on punishing cheaters doing impersonation using computer resources.

2. **Indian Penal Code (IPC) 1980**

Identity thefts and associated cyber frauds are embodied in the Indian Penal Code (IPC), 1860 - invoked along with the Information Technology Act of 2000. The primary relevant section of the IPC covers cyber frauds:

Forgery (Section 464)

Forgery pre-planned for cheating (Section 468)

False documentation (Section 465)

Presenting a forged document as genuine (Section 471)

Reputation damage (Section 469)

3. **Companies Act of 2013**

The corporate stakeholders refer to the Companies Act of 2013 as the legal obligation necessary for the refinement of daily operations. The directives of this Act cement all the required techno-legal compliances, putting the less compliant companies in a legal fix. The Companies Act 2013 vested powers in the hands of the SFIO (Serious Frauds Investigation Office) to prosecute Indian companies and their directors. Also, post the notification of the Companies Inspection, Investment, and Inquiry Rules, 2014, SFIOs have become even more proactive and stern in this regard. The legislature ensured that all the regulatory compliances are well-covered, including cyber forensics, e-discovery, and cybersecurity diligence. The Companies (Management and Administration) Rules, 2014 prescribes strict guidelines confirming the cybersecurity obligations and responsibilities of the company directors and leaders.

4. **NIST Compliance**

The Cybersecurity Framework (NCFS), authorized by the National Institute of Standards and Technology (NIST), offers a harmonized approach to cybersecurity as the most reliable global certifying body. NIST Cybersecurity Framework encompasses all required guidelines, standards, and best practices to manage the cyber-related risks responsibly. This framework is prioritized flexibility and cost-effectiveness.

It promotes the resilience and protection of critical infrastructure by:

- Allowing better interpretation, management, and reduction of cybersecurity risks – to mitigate data loss, data misuse, and the subsequent restoration costs
- Determining the most important activities and critical operations - to focus on securing them
- Demonstrates the trust-worthiness of organizations that secure critical assets
- Helps to prioritize investments to maximize the cybersecurity ROI
- Addresses regulatory and contractual obligations
- Supports the wider information security program

By combining the NIST CSF framework with ISO/IEC 27001 - cyber security risk management becomes simplified. It also makes communication easier throughout the organization and across the supply chains via common cybersecurity directives laid by NIST.

Modern-Day Cyber Security Challenges &Issues

Cyber security laws in India are governed by the Information Technology Act of 2000, which was last updated in 2008. And that was nearly a decade ago. Unlike other laws which can be updated in their own time, Cyber-security Laws are obligated to keep up with the rapid changes in the industry. In India, these laws haven't been updated in a long time.

To briefly state what are some of the weaknesses of the existing cyber law in India:

- All Social Networking Sites shall be subject to the IT Act and should allocate a specialized team to respond to requests from Law Enforcement Agencies (LEAs) as quickly as possible.
- In order to provide service to LEAs, all ISPs must keep records for at least 180 days.
- Each district court should establish a special Cyber Court to hear and issue orders in instances that cannot wait for the legal system to catch up.
- Digital Evidence Authenticators should be required to certify digital evidence. This will be accomplished by an autonomous Bureau.
- Websites and services that operate in India should have their own set of rules. This includes services with foreign roots that operate in India.
- Indian residents' personal information should be stored on Indian servers. (In the United States, this is known as HIPAA compliance)
- Payment Banks and Waller Services should be included within the IT Act's tight requirements, which necessitate a 30-day resolution period.

What is the Scope of Cyber Law in India?

Cybercrime, such as phishing, identity theft, and fraud, has skyrocketed in recent years. However, its coverage under the existing laws is neither adequate nor comprehensive. In addition, we are expected to see greater consolidation of cyber crime penetration in India. This emphasizes the importance of developing more effective and deterrent legal frameworks as well as more strict laws for cyber crime.

The National Cyber Security Strategy is one of the most eagerly anticipated breakthroughs in Indian cyber law. This plan aspires to be a complete guiding gospel for individuals, policymakers, and other stakeholders, as well as a follow-up to the National Cyber Security Policy of 2013.

The strategy will most likely shed additional light on the best reaction mechanisms for improving cyber security in government and other industries.

India will need to start working on a separate national cyber security law very soon. The need for such a law is critical since it will be a critical weapon for safeguarding India's cyber security and cyber sovereign interests.

India is slightly behind the curve at a time when many other countries have already begun enacting specialized cyber security legislation. Appropriate action is required in this regard.

Hopefully, the government will focus on more effective measures to tackle cybercrime in the future. It is also hoped that more relevant reforms in Indian cyber law will be made to include enabling legal measures to address the difficulties posed by rapidly emerging technologies.
Final Thoughts As human dependence on technology intensifies, cyber-security laws in India and across the globe need constant up-gradation and refinements. The pandemic has also pushed much of the workforce into a remote working module increasing the need for app security.

Lawmakers have to go the extra mile to stay ahead of the impostors, in order to block them at their advent.

Cybercrimes can be controlled but it needs collaborative efforts of the lawmakers, the Internet or Network providers, the intercessors like banks and shopping sites, and, most importantly, the users.

Only the prudent efforts of these stakeholders, ensuring their confinement to the laws of the cyberland - can bring about online safety and resilience.