

Original Article

India USA and Other Countries Cyber Security Awareness and Laws

Dr. Bindu Kumari

Assistant Professor, Maulana Azad University Jodhpur (Raj.)

Abstract Due to technological advancements and our increasing reliance on devices, cybercrimes are getting more and more prevalent. People's lives are now completely dominated by technology, which has had some very negative effects. Because information is freely shared online, all types of crimes are committed there. As a matter of national security and public welfare, nations are being increasingly watchful of data protection. The degree in which end users is aware from and comprehend cyber security best applies and the daily cyber dangers that their networks or organizations encounter is referred to as cyber security awareness. An attack on crucial data kept on a computer or network is known as a cyber-threat. These assaults let a person or group to obtain personal information without authorization with the goal of stealing or damaging sensitive data, including IT assets and intellectual property. Cybersecurity is the field concerned with preventing fraudulent actions like as theft, phishing, trojan horses, malwares assaults, unlawful access to data, & damage to internet networks and data. Because of the growing reliance of people, corporations, and governments on the internet, maintaining the confidentiality of digital assets is crucial for cyber security. This study examines the current laws pertaining to cyber laws. Its goal is to draw attention to the US, U. K. Kingdom, & India—three countries that is well-known for their active involvement in the field of cyber security.

Keywords: - Cyber Crimes, Cyber Laws, Awareness Cyber, Cyber Security.

Address for correspondence: Dr. Bindu Kumari, Assistant Professor, Maulana Azad University Jodhpur (Raj.), Q.no 3685, Bank Note Press colony, Dewas (M. P.) Pin-455001

Email: yadavbindu130@gmail.com

Submitted: 19 June 2024 **Revised:** 1 July 2024 **Accepted:** 15 July 2024 **Published:** 31 Aug 2024

INTRODUCTION:-

Cyber security wakefulness entails the ongoing effort to educate students and employees about the potential dangers present in the digital empire and how to consistently respond to them. The primary factor behind this phenomenon is the emergence of new risks and advancements in technology.

According to Dr. Bruce, the study supporting the index will help reveal the true identities of cyber-criminal offenders, and we anticipate that it will assist in combating the increasing danger posed by profit-motivated cybercrime⁽¹⁾.

OBJECTIVE:-

1. The main aim of this study is to emphasize the countries that are generally recognized for their active participation in cyber security, notably the US and India.
2. For understanding various types of Cyber threats.
3. Developing cyber security best practices.
4. To gain practical knowledge and skills to identify and mitigate cyber threats effectively.


METHODOLOGY OF DATA ANALYSIS:-

The data gathering procedure includes using the secondary data approach. This will entail exploring numerous websites, publications, journals, and other materials for relevant information. The secondary data will be applied to study the prevalence of different cyber crimes in both India and western countries.

• WORLD - FIRST "cyber crime index" ranks country cyber crime threat level

The Index, released today in the Journal PLOS One, indicates that a select few countries harbor the most significant cyber criminal menace. Russia is ranked first, followed by Ukraine, China, the USA, Nigeria, and Romania. The United Kingdom ranks eighth.

According to Miranda Bruce: - The study showed by the University of Oxford and the Australian National University (ANU) in Canberra could enable the public and private sectors to assign their resources more effectively by targeting major cybercrime centers.

Quick Response Code: 	Access this article online
	Website: https://rlgjaar.com
	Website: https://www.doi.org DOI: 10.5281/zenodo.14059803

This is an open access journal, and articles are distributed under the terms of the [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/). The Creative Commons Attribution license allows re-distribution and re-use of a licensed work on the condition that the creator is appropriately credited

How to cite this article:

Kumari, D. B. (2024). India USA and Other Countries Cyber Security Awareness and Laws. Royal International Global Journal of Advance and Applied Research, 1(2), 32–36. <https://doi.org/10.5281/zenodo.14059803>

This will reduce the need for extensive investments in cybercrime countermeasures in countries where the problem is less prevalent.

The index's data was gathered via a poll of 92 notable cyber crime professionals worldwide who are actively engaged in the collection of cyber crime intelligence and conducting investigations. The survey

requested experts to evaluate five primary categories of cybercrime, identify the countries they deemed to be the most significant originators of each type of cybercrime, and subsequently rank each country based on the impact, professionalism, and technical expertise of its cybercriminals.

CYBERCRIME INDEX

(Ranking countries by cyber crime threat level)

Ranking	Country	WC Score
I	Russia.	58.39
II	China.	27.86
III	Ukraine.	36.44
IV	United States.	25.01
V	Nigeria.	21.28
VI	Romania.	14.83
VII	North Korea	10.6
VIII	United Kingdom.	9.011

According to Cyber crime index:-

India has 10th rank in cybercrime (16 April 2024)

SIGNS OF SPOOFING

1. The sender's email address closely resembles the original.@
2. Poor grammars are used in the given messages. (name)

3. The appear URL address does not include the "s" in the https://

4. You receive many calls from unknown numbers.



5. Attachments in emails seem suspicious.



How to protect against Spoofing attacks:-

Dos:-
<ul style="list-style-type: none"> • Turn the your spam filter. • Grammar Check. • However over the URL before clicking • Confirm information with source • Set up two- factor authentication • Download cyber security software.

Don't s:-
<ul style="list-style-type: none"> • Click the familiar downloads • Respond to phone calls or emails from unfamiliar senders. • Do not disclose your personal information to strange sources. • Utilize a single password for various login credentials.

Cyber Crime :-

Cybercrime refers to criminal activities are carried out using a computer, network, or network device. The phrase "cyber-crimes" is not explicitly clear in any legislation or legal framework in India. The term "cyber" is frequently used within the domain of various computers. Cybercrimes have the capacity to impact many different people⁽²⁾.

Types of Cyber crimes :-

During the Covid-19 pandemic, there have been a significant shift in the developmental patterns of persons, migrating from offline-to-online activities. In 2022, thieves are expected to target a lucrative sum of 7.1 trillion, an enormous rise from the 1.2 trillion recorded in 2019. Cybercrimes are prevalent Not only in India, but also in Western nations such the USA, UK, Germany, even Russia.

Phishing :-

Typically, it is accomplished by email. The main goal is to get sensitive data, like credit card & login details, or to installing malware on the target's

device. The process commences with a deceitful email or other form of communication that is specifically crafted to deceive the recipient. In rare cases, malicious software may also be downloaded into the victim's computer. Phishing refers to the malicious practice of deceiving consumers into engaging in harmful actions, such as clicking on links that are malicious that will install malware or redirecting them to an untrustworthy website. According to the research findings, India experienced over 79 million instances of phishing attacks in the year before this one. The population of the USA is 1.1 billion, while the population of the UK is 112.9 million.

Examples of Phishing attack :-

The email notifies the user that their password is about to expire and provides instructions to visit myuniversity.edu/renewal in order to renew their password within a 24-hour timeframe.

Ransom ware :-

Ransomware is a form of cryptovirological malware that effectively prevents individuals from

accessing their personal data until they pay a ransom. The exchange rate or pricing rate fluctuates based on the particular form of Ransomware. In April 2024, there was significant activity related to Ransomware, as depicted in the accompanying image that illustrates the changing patterns among the five most active organizations. In April 2024, hunters noticed a substantial rise in the number of prey, indicating a 66.67 percent increase compared to March.

In 1989, Joseph L. Popp, an evolutionary biologist with a Harvard education, developed the first-ever ransomware virus.

Cyber pornography :-

According to section 67 of the Information Technology Act, 2000, it acts as a crime to create, transmit, or distribute cyber pornography. Cyber pornography involves the use of the internet to produce, show, distribute, import, or publish explicit materials, particularly those representing children involved in sexual activities through adults. Phrase "photography" refers to the act of depicting sexual acts in books or films with the intention of causing sexual arousal. This practice is commonly associated with providing immediate gratification or appealing to the younger generation, while the older generation views it as a violation of cultural, ethical, and moral values.

Cyber terrorism:-

By utilizing the internet, individuals engage in violent activities that lead to or pose a danger of loss of life. Cyber terrorism is synonymous with digital terrorism⁽³⁾.

Examples of Cyber terrorism:-

1. Server hacking to steal sensitive information.
2. Virus introduction of data networks.
3. Making websites inaccessible by ruining them.
4. Engaging in acts of terrorism by targeting financial institutions with the intention of illicitly transferring money.

Cyber Stalking:-

Anyone who possesses a Smartphone, social media profile, or GPS connected gadget is susceptible to becoming a victim of Cyber stalking. At present, internet stalking has become more prevalent compared to in-person stalking. Females between the ages of 18 and 30 are the most probable targets of cyber stalking, which occurs due to sentiments of hatred, vengeance, or even lust.

Cyber law legislation in Ind.:-

Information Technology law 2000:-

The major legislation in India that addresses cyber crime and internet trade is the statute in question. This act is made public on 17 October. An act to establish legal validity for transactions conducted through digital exchange of data and other forms of electronic communication. This legislation safeguards online users from identity theft, financial harm, and other serious cybercrimes by implementing legal procedures to supervise and regulate the actions of computer devices that connect to the Internet. The parliament of

India passed this law in order to safeguard the domains of e-commerce, e-governance, and e-banking, while also addressing sanctions and punishments related to cyber crimes⁽⁴⁾.

There are some provisions of the act:-

- **Section 65-** Modifying computer materials from sources. Computer source code includes the compilation of programmers' instructions, computer layout and design, and the analysis of program resources. Intentionally destruction, concealing, or changing the source code is regarded as an infraction and may result in a punishment of up to 3 years of prison or a fine of 2 Lakhs INR, or both.
- **Section 66 :- Another person's password uses** - Illegally employing someone individual's password, digital signature, or any other distinct identifier can lead to a prospective prison sentence of 3 years or a fine of one lakh INR.
- **Section 66d:- Cheating through various computer resource:-** Engaging in cheating through using a computer resource or a communication device is considered an example of cyber crime. The offense carries the punishment of imprisonment for a maximum time frame of 3 years or a fine of up to 1 Lakh INR.
- **Section 66E :- Publication of sensitive images of others** - The act of taking and posting explicit photographs of someone's intimate organs without their consent or knowledge is regarded as a cybercrime. The act is subject to legal consequences, with the offender potentially receiving a jail sentence of up to 3 years and a fine of up to 2 lakh INR, or both.
- **Section 66 F:- cyber terrorism acts** - Unauthorized people who attempt to access a computer resource without permission, with the goal of damaging the integrity, security, unity, and sovereignty of the nation, may face life imprisonment. This section deals to a non-bailable offense.
- **Sections 67 :- Child Related Pornography** - Impose penalties for distributing or transmission of sexually explicit content involving children in electronic format. Sections 13 to 15 of the Protection of Children from Sexual Offences (POCSO) Act additionally include strict penalties for child pornography. Distributing pictures depicting a minor performing sexually explicit conduct is an offense that carries the maximum prison sentence of 7 years, a fine of up to 10 lakh INR, or both.
- **Section 69:-** Government's authority to restrict access to web/sites
 1. Protection of India
 2. State security.
 3. To prevent
- The government possesses the authority to make directives to safeguard the sovereignty and integrity of India. Under section 69A, the government has the right to snatch, detect, or

access any data that is acquired, transmitted, established, or stored in computer resources. Additionally, the central government has the power to prevent public contact to any data.

- **Section 43A - Corporate level Data Protecting:** - If the corporate entity miscarries to properly appliance safety protocols, resulting in harm or financial gain to an individual, that corporate entity has a responsibility to provide reward to the injured party.

NCS (National Cyber security) policy, 2013:-

The Indian government implemented a revised framework in 2013 to safeguard against cyber threats. This legislation has been enacted. This statute additionally offers a basis for secure and reliable electric communications. The nationwide Cybersecurity strategy provides a roadmap for establishing a comprehensive, collaborative, and communal framework to effectively address the challenges of cybersecurity from all levels inside the nation⁽⁵⁾.

Few objectives of this policy are :-

1. To develop a the better cyber ecosystem in IN.
2. To set up and sustain a central authority for managing cyber-attack emergencies.
1. **National CyberSecurity Strategy 2020:-** The implementation of cybersecurity measures is becoming prevalent in both the public and commercial sectors. The Government of India has just introduced the National Cybersecurity Strategy for the year 2020. Their objective is to enhance cyber awareness and cyber security by conducting more rigorous audits. Disciplinary regulations and latest legislation are crucial for keeping up with the constant advancements and changes in technology.

There are some foundation of strategy :-

1. Ensuring the safety and protection of the national cyberspace.
2. Achieve synergy by integrating people, processes, and capabilities.
3. Enhance the efficacy of resources such as teamwork and collaboration.
2. **National Cyber security strategy 2021:-** The National Cybersecurity Strategy is a detailed blueprint that outlines a nation's strategy for safeguarding its digital infrastructure, data, and systems from cyber threats. The 2021 regulations also mandate that intermediaries must inform the CERT - IN about any security breaches as part of their responsibility to exercise due diligence.
3. **National Cyber security policy 2022:-** The research concentrated on 21 domains to ensure the safety, security, reliability, resilience, and dynamism of India's cyberspace. The new National Cybersecurity Strategy of 2021 adopts a comprehensive approach to tackle the issue of cybersecurity in the digital realm.
4. **National Cyber security policy 2023:-** The primary objective of this policy is to enhance the technical, physical, and logical aspects of

Cyberspace in order to facilitate the development of a robust cyber security framework and safeguard key information infrastructure. To do this, the policy established a national Cyber security agency.

5. **National Cyber security policy 2024 :-** The Department of Defense's cyber security policy for 2024 prioritizes enhancing engagement with the Defense Industrial Base (DIB) by implementing pilot programs in the field of cyber security. It improves the capacity to prevent and address cyber attacks. The combination of institutional structures, individuals, processes, technology, and cooperation aids in mitigating risks and minimizing the impact of cyber incidents.

Cyber law legislation in USA

Federal Trade Commission Act (FTCA) in the United States of America outlaws deceptive acts and practices in business, particularly those pertaining to data security.

The Cybersecurity & Assets Security Support (CISA) is responsible for spearheading the nationwide initiatives aimed at comprehending, overseeing, and mitigating risks to our cyber and physical assets⁽⁶⁾.

Below are several significant provisions :-

1. **The country fit access scheme and computer scam and abuse act 1984:-** The United States of America is currently grappling with a significant volume of cyber attacks and cyber crimes. The legislation governing cyber security in the country is intricate. This legislation aims to protect computer systems that contain confidential information related to international trade and global e-commerce, which are owned by government and interstate entities.
2. **The computer security at 1987:-** The NIST has been established with the assistance of this agency. The primary goal of this agency is to enhance the security system and uphold stringent security standards. The aims of this act are to mitigate cyber crime and promote cyber awareness. However, it does not apply to military and defense affairs.
3. **The cyber security research development act, 2002 :-** The purpose of this act is to establish a research agency. The objective of this agency was to mitigate cyber threats while simultaneously enhancing the infrastructure in a specific state of America. The responsibility for this purpose, namely the National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST), has been assigned to the school.
4. **E- government act 2002 :-** This legislation is of utmost importance. This legislation imposes stringent regulations that must be adhered to in order to ensure cyber security throughout the nation. This legislation also establishes the structure for federal information technology. Currently, the United States government is

actively enhancing cyber security legislation by revising existing laws and enacting new ones.

Examples of such laws are :-

- **Federal exchanges data bridge notification Act, 2015 :-** This act aims to establish norms for the health assurance business in provinces. From this act any data breach must be reported within 60 days of its occurrence. In addition, victims of such breaches are entitled to compensation. Non-compliance with this clause can result in severe penalties under the legislation.
- **Cyber security information sharing Act, 2015 (CISA):-** For the purpose of exchanging information among multiple federal entities operating within the country. The primary objectives of this Act are to facilitate the prompt transfer of cyber security issues, glitches, and other related problems⁽⁷⁾.

Cyber security Laws in United Kingdom:-

The UK general data protection regulation needs personal data be processed securely, using suitable technical and organizational measures. The regulations pertaining to consumer protections against hacking and cyber attacks will come into effect. Several significant acts are now in effect in the UK to safeguard against cyber crimes.

- **Penalty of noncompliance with provisions of act-** The amount is 17.5 million euros, which is equivalent to 4% of the yearly global turnover.
- **U.K. General data protection regulation (UK-GDPR)-** The rules and regulations regarding the protection of personal data apply from all countries of the United Kingdom, including England, Wales, Scotland, and Northern Ireland.
- The penalty for failing to comply with the rules of the UK-GDPR can result in a fine of up to £20-21 million or four percent of the company's annual revenue⁽⁸⁾.

CONCLUSION:-

The United States, the United Kingdom, and India have different legal, cultural, and technological environments, which appear in their individual cyber security legislation, such as the Information Technology Act 2000 and the National Cyber Security Policy. These measures have made substantial advancements towards improving cyber security in India. There are present worries surrounding how to allocate of resources, execution, and the dynamic nature of cyber threats. Data security and individual privacy are major considerations in all three countries.

Acknowledgments

The author is thankful to Dr. Iname llahi, Dean of Social Science and Humanities, Maulana Azad University, Jodhpur for granting permission to carry out the work.

Financial support and sponsorship

Nil.

Conflicts of interest

There are no conflicts of interest.

REFERENCES :-

1. Federal laws Relating to cyber security: overview of major issues, current laws, and Proposed legislation, available at <https://fas.org/SGP/crs/natsec>
2. Yoshita Gandhi, "cyber laws: Comparative study of Indian law & Foreign laws," 1 journal of applicable law & jurisprudence 10
3. Singh Anand K. "Cyber Crime, Law and Social Challenges", in Neeraj K.Rai (Ed.) Social Media: Issues and Challenges, Avon Publishing House, Delhi,2020
4. Cyber crime, available at: <http://www.byjus.com> (last visited on November 3 2023)
5. Phishing attacks: Defending your organization, available at: <http://www.ncsc.gov.uk>
6. Sieber Ulrich, The International Emergence of Criminal Information Law, Information Technology Crime, Kolu, 1992.
7. Ransom ware available at: <http://en.wikipedia.org>
8. Richard C. Hollinger, "Computer Crime" in Clifton D. Bryant (Ed.).