International Journal of Advance and Applied Research
www.ijaar.co.in
ISSN – 2347-7075 Impact Factor – 7.328
Peer Reviewed Bi-Monthly
Vol.9 No.6 July – Aug 2022

SOCIO-LEGAL ISSUES OF CYBER SECURITY IN INDIA

Dr. Jahdav N. D.
Assistant Professor, Dayanand College of Law, Latur
***Corresponding Author*- Dr. Jahdav N. D.**
Email Id- jadhavnd1@gmail.com
DOI- 10.5281/zenodo.7064576

Introduction:-

Cyber security is the protection of internet connected systems such as hardware, software & data from cyber-threats. The practice is used by individuals & enterprises to protect against unauthorized access to data centers & other computerized systems. With an increasing number of users, devices & programs in the modern enterprise, combined with the increased deluge of data much of which is sensitive or confidential the importance of cyber security continues to grow. The growing volume & sophistication of cyber attackers & attack techniques compound the problem even further. An effective cyber security method has numerous layers of defence spread across the networks, computers programs or information that one aims to keep non-toxic. In a society, the processes, the people & tools must all accompaniment one alternative to generate a real defence on or after cyber-attacks.

Meaning:

The technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems form malicious attacks is known as cyber security.

"Cyber security is the set of principles & online information against threats".[1]

Types of Cyber security:-

1. Malware is a form of malicious software in which any file or program can be used to harm a computer user.
2. Ransom ware is another type of malware. It involves an attacker locking the victim's computer system files.
3. Social engineering is an attack that relies on human interaction to trick users into breaking security procedures to gain sensitive information that is typically protected.
4. Phishing is a form of social engineering where fraudulent email or text messages that resemble those from reputable or known sources are sent.
5. Spear phishing is a type of phishing attack that has an intended target user, organization or business.[2]

History of Cyber Security:-

Cyber security is the practice of protecting computers, mobile devices & data from malicious attacks. The first cyber malware virus developed was pure of innocent mistakes. But cyber security has evolved rapidly because of the impeccable increase in the cybercrime law filed on the web. As these time-sharing systems emerged in the mid to late 1960 & many more jobs are using web, users were able to run at a similar time, controlling the access to data on the systems became a major point of concern. The cyber security checking began in the 1970, when researcher Bob Thomas created a computer program caused creeper that could move across ARPANET's network.

Ray Tomlinson, the innovator of email wrote the program Reaper, which chased & deleted creepers. In 1971, programme. Bob Thomas made history by innovated a program that is widely accepted as the first incident ever

[1] www.javatpoint.com

[2] www.techtarget.comcdn.ampproject.org

computer Trojan as the worm & Trojan bounced between computers PC, which has ground breaker at that time. The year 1987 was the birth year of commercials malware examining antivirus. In the early 2000 criminal organizations stated to heavily fund professional cyber attacks & governments began to clamp down on the criminality of hackings, giving much money serious sentences to those culpable hackers & information security continues to advance as the internet grows as well but, unfortunately so having the viruses. The cyber security industries are continuing to grow. The most global cyber security market size is forecast to grow to $345.4 bn by 2026 according to statist tic.[3]

Issues of Cyber Security:-

As the ability to access cyberspace expands due to tech innovations, the number of cyber security issues organizations may face also grows.

Organizations & Cyber Security Attacks:

Cyber security attacks can happen to any organization at any time. In the year 2020, established organizations such as Marriott, MGM Resorts, Twitter & Magellan Health all fell victim to cyber attacks. Preventing these attacks is financially critical. There are several different cyber security issues to be aware of in today's business landscape-issues that only a seasoned cyber security professional may be able to help prevent.

Social Engineering:-

It represents a catch all term for various tactics that are used by hackers. These tactics are designed to trick individuals into giving out sensitive. According to security software company digital guardian, phishing represents 91% of social engineering attacks.

Ransom ware:-

It is another tactic used by hackers. The objective is to hold a company's data hostage until the affected user pays a specific dollar amount, which can often be hefty.

Cloud Computing issues:-

Cloud storage & the internet of things have exposed new vulnerabilities. Organizations & businesses must make security plans that take new security threats into consideration, rather than only protecting business computers & mobile devices.

Distributed denial of service:-

The hallmark of these attacks in coordination of cyber attacker floods the system with a high number of simultaneous functions, such as a request to a webpage.

Artificial intelligence & machine learning:-

In the hands of cyber criminals, artificial intelligence & machine learning can enable cyber attacks to become more sophisticated & efficient.

vii. Crypto & Block chain attacks:-

Those looking to use block chain in their business should take great care to make sure their cyber security strategies include protection for these emerging, evolving markets.[4]

Legislative Measures for Cyber Security:-

1.The Indian Penal Code, 1860:-

The IPC, 1860 contains provisions dealing with the menace of cyber defamation.

1. Section 499- Defamation
2. Section 469- forgery for purpose of harming reputation.
3. Section 470- forged document or electronic record.
4. Section 503- criminal intimidation.

2. The Information Technology Act, 2000:-

This Act is to protect the field of e-commerce, e-governance, e-banking as well as to provide for penalties & punishment in the field of cyber crimes. This Act further amended by the Information Technology Act, 2008.

The amendment has replaced section 43 by section 66. Section 43-A & Section 72-A were added to the IT. Act, 2008. The Information Technology Rules, 2011 were notified by the Indian Government under section 43-A of the IT. Act.

[3] https://www.geeksforgeeks.org

[4] online.maryville.edu

The Indian Insurance Regulatory & Development Authority has put in place several guidelines including IRDA guidelines on Information & Cyber Security for Insurers, Regulations 2017, pertaining to data security & application on Insurers.[5]

3. Companies Act of 2013:-

The legislature ensured that all the regulatory compliances are well-overed, including cyber forensics, e-discovery & Cyber Security diligence. The companies (management & Administration) Rules, 2014 prescribes strict guidelines confirming the cyber security obligations & responsibilities of the company directors & leaders.[6]

Judicial Approach towards Cyber Security:-

State of Tamil Nadu vs. Suhas Kutti[7]

The accused held guilty of offences under section 469, 509 IPC & 67 of IT Act 2000, sentenced for the offence to undergo rigorous imprisonment for two years.

2. Avinash Bajaj vs. State (N.C.T) of Delhi[8]

The famous Bazee.com case, the CEO Avinash Bajaj was arrested for an advertisement by a user to sell the DPS Sex Scandal video. The video was not uploaded on the portal despite that accused was arrested u/s. 67 of IT. Act. The court ordered accused to surrender his passport & not to leave India without permission of the court.

3. Shreya Singhal vs. Union of India[9]

S. 66A of the IT. Act 2000 was struck down by the SC. as unconstitutional.

4. SMC Pneumatics (India) Pvt. Ltd. Vs. Jogesh Kawatra

In this case Court granted an ad-interim injunction & restrained the employee form sending, publishing & transmitting e-mails which are defamatory to the plaintiffs.

Conclusion:-

Cyber security is a complex subject, whose understanding requires knowledge & expertise from multiple disciplines, including but not limited to computer science & information technology, psychology, international relations & law. In practice, although technical measures are an important element, cyber security is not primarily a technical matter, although it is easy for policy analysts & others to get lost in the technical details.

[5] https://www.ripublication.com
[6] https://www.appknox.com
[7] AIR 2004 SC 4680
[8] AIR (2008) 105 DRJ 721
[9] AIR 2015 SC 1523