Unit 1: CyberSecurityIssues and Challenges

Structure

1.0 INTRODUCTION

Information Technology is a dual edged sword. It is can be used for the betterment of mankind like in telecommunications, governance, public health, education, research, finance etc. but may also be used for disruptive purposes. Cyber security provides protection against use of information technology for disruptive purposes. This cyber security is nothing but technologies, processes, practices to protect computers, computer networks, and computer systems from cyber-attacks. In addition to technology there are certain laws which penalise commissions and omissions posing threat to cyber security.Remedies provided by laws include compensation, imprisonment, forfeiture, fine etc. Primary legislation regulating information technology is Information Technology Act 2000 and allied rules and regulations. The Information Technology Act 2000 defines and prescribes punishment for acts and omissions which poses threat to cyber security. The Act provides long arm jurisdiction meaning there by Courts in India have jurisdictions against the perpetrators of cyber offences not only residing in India but also in foreign countries. The Act also provides for the definition of cyber security under Section 2(nb) which states that cyber security is protection of information, devices, equipment, computer, computer resource, communication device as well as information stored from any use, un-authorized access, disclosure, disruption, modification and destruction(**IT act, sec2, https://www.indiacode.nic.in/).** Due to increasing cybercrimes, countries have become more aware of such exploitation and are taking necessary steps to curb exploitation by protecting their data through 'cyber security' from getting exploited.

1.1 OBJECTIVES

After studying this unit, you should be able to:

- Explain the meaning and need of cyber security.
- Explain pros and cons of digital security
- Discuss ways in which cyberspace security is breached
- Explain technologies which can play significant role in providing cyber security
- Explain laws which aim at protecting cyberspace and prescribe penalty or punishment for those who pose threat to cyber security

1.2 DIGITAL SECURITY: PROS & CONS

Digital security is a broader term which encompasses within itself protection of online identity data assets Technology with the use of various tools like software, Web Services, biometrics, firewalls, proxies, vulnerability scanner, instant message or telephone encryption tools etc. Digital security provides protection against cyber-attacks unauthorised access, online malicious activities etc.

The 3 pillars of digital security are**(Mark Burnette, 2020, p.1**):

1. Confidentiality
2. Integrity
3. Availability

The basic essence of these principles is that the information which is private should be shared with the least amount of people to keep it more secure, the information provided should not be modified or corrupted and lastly, that the information provided should work effectively and efficiently at all times.

The OECD Recommendation and its companion documents were published in 2015 which provides guidance for all stakeholders on cyber security aspects. The Organization for Economic Cooperation and Development (OECD) helps in facilitating information, data and is progressing to eradicate poverty and inequality by bringing forefront solutions for the benefit of the world. The OECD Working Party on Security and Privacy in the Digital Economy (SPDE) develops public policy analysis and high-level recommendations to help governments and other stakeholders to ensure that digital security and privacy protection foster the development of the digital economy. (**OECD, 2015, p1)**

1.2.1 Digital Security: Pros

- It helps in protecting personal information stored in devices.
- Suspicious or unauthorized access to devices can be blocked through digital security and thus preventing possible harm.
- Security based on biometrics is capable of providing a higher degree of protection against attacks as it's difficult to steal biometric information.
- Digital security enables oneself to fearlessly communicate, transact, work etc. in online mode.
- Protects the computer from crashing or slowing down and thus protects business, transactions, communication etc. happening over computer, network or system

- Digital security thus may help in fostering the economy of the State as it cuts down on many costs.

1.2.2 Digital Security Cons

- Availing services or procuring tools for digital security can be a costly affair.
- Web services or tools may or may not be compatible with the device of the user.
- Digital security services or tools may be difficult to configure at times and needs to be updated regularly
- Services or tools may slow down functioning of user's device or at times may intervene even normal functioning of another programme

Please answer the following Check Your progress.

Check Your progress 1 *Spend 3 Min*

Write any three benefits of Digital Security?

1.3 SECURITY ISSUES /BREACHES IN CYBERSPACE

"Cyber Space" can be defined as a virtual space or to be more specific an electronic medium that is used to facilitate exchange of ideas via electronic means. The crimes which take place in the cyber space are termed as "cybercrimes".

A 'cyber incident' is defined under the section 2(e) of the CERT Rules as "any real or suspected adverse event that is likely to cause or causes an offence or contravention, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, systems, services or networks resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource, changes to data or information without authorisation; or threatens public health or safety, undermines public confidence, have a negative effect on the national economy, or diminishes the security posture of the nation".(**Ministry of Electronics and Information Technology Notification, 2018, p6**)

Threats to cyber security have been evolving from time to time and newer threats seem to emerge day by day. It's difficult to cover all of them however following are the most common security issues witnessed in cyberspace in recent past.

1. **Unauthorised access**– It is accessing computer, computer, network, system or device without permission from those who are authorized to access the same.

   Eg. Mr. Shyam spies on Ms. Rita and gets to know unlocking pattern set on her mobile device. Then Mr. Shyam without permission of Ms. Rita access pictures stored in her mobile device. This is an unauthorized access. Another example would be Mr. Shyam knows email address of Ms. Rita but not password. He tries different permutation and combination of passwords and finally gets access to all the emails

received by Ms. Rita. Unauthorized can be in the physical form too. Let's say Ms. Rita without permission from Ms. Shyam steals his pen drive and then accesses data stored in it. This acts also amounts to unauthorized access. Similarly stealing credit/debit card and then trying to use it for siphoning someone else's money involves element of unauthorized access.

2. **Distributed Denial of Service Attack** - It is aimed to adversely affect functioning of a website by sending multiple requests to a website which is beyond its control to handle. It's an attack on a machine or network resource to make it unavailable to intended users by flooding it with unnecessary traffic.(**GOsafeonline (2014**). Mr. AB creates a botnet herd which upon the command from control and command server sends huge amount of data to a server hosting a banks website resulting slowing down of the website. This is an example of denial-of-service attack on the bank.

3. **Malwares** - Malwares are software which are designed to harm network or device. It includes Botnets, Ransomwares, Trojan, Virus, Worms, Spywares etc. Botnets are collections of devices connected through the internet and infected with malware so the same may be controlled to carry out cyber-attacks. Ransomwares are malwares which encrypts files, data etc of the victim and then demands ransom from the victim to decrypt or permit access to files or data. Trojan is a malicious software which prima facie looks legitimate but is intended to steal, harm, damage device of victim. Term trojan has been picked from an ancient Greek story where a large structure resembling a horse was used to lead an attack against the city of Troy. Virus is a malicious programme which is designed to affect the functioning of a computer/device in which it is executed and capable of spreading from one computer to another. Virus is a malicious programme capable of self-replicating and spreading across networks. Spywares are malicious software which are installed in victims' devices without his knowledge to secretly spy and gather information of victims.

   Eg. One of the most infamous malware till date is ILOVEYOU malware spread in the year 2000. The mail prompted the victim to download 'LOVE-LETTER-FOR-YOU.TXT.vbs' attachment. The malware was in fact a worm and it overwrote system file and personal files of those who ended up downloading them.

4. **Social Engineering attacks** - These attacks harp upon psychological manipulation of victims and tricking the victim into revealing sensitive information. The victim is tricked to click on a malicious link or respond to fraudulent mail etc.

5. **Phishing** - It's an activity by which the victim is deceived to reveal sensitive information like username, passwords, credit/debit card details etc by disguising oneself as a trustworthy entity. Coining of term 'phishing' is inspired from term fishing as in fishing, bait is cast to fool fishes similarly deceiving message/mail/webpage is cast to fool innocent online user. Eg. Employee Ms. CD apparently receives a mail from Finance Officer of the Company in which she is working. The mail is in fact sent by an imposter who has disguised himself/herself as Finance officer.

6. **Crypto jacking** - It is unauthorised use of victims' device to secretly mine crypto currency. Crypto currency is a virtual currency with no central regulatory or issuing authority and secured through crypto currency. Crypto jacking affects the functioning

of devices as the same takes a toll on the device. For e.g Malwares use CPU's for mining crypto currency.

7. **Exploiting vulnerability**- Vulnerability is a flaw in the measures taken to secure a device. Such flaw is exploited by the attacker to gain access over the device or harm it.

8. **Cyber physical attacks** - These are cyber-attacks breaching the security and impacting the physical environment. This may include shutting down of cameras, lights etc. which are cyber controlled.

   E.g. Cyber attacker takes control over water pumps controlled by technology and causes destruction to property. Attacker taking control over cooling systems in nuclear reactor has the potential to inflict tremendous harm and pose threat to national security and safety.

9. **Internet of Things (IOT) attacks** - Embedded devices that are connected to a network and capable of transferring data are at the risk of being attacked through exploiting vulnerability and can be hacked.
   For e.g., Fax machines connected to internet may be exploited with their vulnerability and data can be stolen.

10. **Web Jacking** - Web jacking a term inspired from hijacking, means hijacking a website or its access and control is taken over by the attacker. This taking over is then misused for tricking the visitors of a website or deface the website.

11. **Drive by download** - A legitimate website is compromised and when the victim browses such a compromised website, the same installs malicious payload in the victim's device. This malicious payload can be in the form of ransomware.

    Some of the common security issues witnessed in cyberspace in recent past are as follows: (**Dr S.R. Myneni, p472-473**).

    1. **Internet time theft**: This involves usage by unapproved persons of the internet hours paid for by another person.

    2. **Key Loggers**: It is a software database or a program intended to covertly keep an eye on and log all keystrokes. The Key logger software scans computers, their processes, and data, the moment a person hits a key on the keyboard. This information is straightaway transmitted over to an external control.

    3. **Website defacement**: This is usually transmitted by the replacement of the homepage of a site by a system cracker that dislocated into a web server and modifies the hosted website creating one of its own. The attacker usually replaces the site matters with his own message or completely destroys the site's contents.

    4. **Pharming**: This takes place when the attacker redirects a user from an authentic and genuine site to a fake and deceitful site where their systems are infused with malware.

5. **Phreaking**: This refers to people who interfere with systems of telecommunication such as public networks.

6. **Email bombing**: This refers to forwarding a significant large number of emails to the victim resulting in the victim's email account or mail servers to not respond.

Check Your progress 2 *Spend 3 Min*

What is Phishing and whether it is challenge to digital security?

1.4 TECHNOLOGY'S ANSWERS TO CYBER SECURITY

1. **Unauthorised access** - Strong passwords, endpoint security, two factor authentications, physical security practices, monitoring user activity are few of the common practices employed for protection against unauthorized access.

2. **Distributed Denial of Service Attack** – Various infocom security tools are used to protect against DOS Attack like anti malware, firewall, spam filtering, switches and routers, Intrusion prevention systems, DDOS defence systems, content delivery network etc.**(GOsafeonline,2014)**

3. **Malwares** - a. Botnets - VPN, secured network architecture, traffic management tools etc. can help in detecting and preventing botnet attack. b. Ransomwares - Backing up data, disabling unnecessary ports or services such as RDP can help in preventing ransomware attack c. Trojan - robust firewall, anti-spywares, maintaining cyber hygiene are helpful against trojans d. Virus - Malware removal software, automatic scans can reduce the risk of virus attacks, e. Worms - Internet connection firewall, network intrusion detection software, use of Domain Message Authentication Reporting (DMARC), Domain Name System Security Extension (DNSSEC) can be helpful. f.

4. **Spywares** - Anti spywares, sandbox protection, ad pop up blockers can play significant role in averting spywares.

5. **Social Engineering attacks** – network traffic analysis, firewalls, updated software, spam protection guards, updated blacklists(**Chizari, Hassan &Zulkurnain, et al (2015**) can aid in preventing social engineering attacks. However, it is considered that the most efficient way to tackle social engineering attacks are awareness about such attacks. Social engineering attacks thrive on people's ignorance and hence awareness is the key to fight against such attacks.

6. **Phishing** - SPAM filters, web filters, patching, use of SSL certificate to secure traffic are a few technologies which may assist in combating Phishing attacks.

7. **Cryptojacking-** anti crypto mining extensions, endpoint protection, web filtering tools, network monitoring solutions etc are helpful in preventing crypto jacking.(**Micheal Nadeau,2021),**

8. **Exploiting vulnerability** – Patching operating systems, enabling SMB signing, network segmentation which limits access to systems etc. may reduce the chances of exploitation of vulnerability.

9. **Cyber physical attacks**- Adequate control on physical access, cyber nodes, enabling remote access only when necessary, two factor authentications etc. are few of the practices which have turned out beneficial in combating cyber physical attacks.

10. **IOT attacks** - Firmware updates with cryptographic signatures, proper identity management, hardened toolchains, libraries and framework, etc may be used for protection against IOT attacks.

11. **Web Jacking** - Web Server firewalls, X frames options etc may be used to prevent web jacking.

12. **Drive by download** - Updating website components, web security software etc. can provide protection against drive-by download.

1.4.1 Cyber Security Intrusion Detection

Intrusion detection systems monitor traffic and generate alerts in the case of suspicious activity tending to harm the cyber security. However, some intrusion detection systems are capable of even prevention of cyber threats. Such intrusion systems may be network, host, hybrid, application, protocol based and method of detection may be signature based or anomaly based. Signature based intrusion detection system detects intrusions based on patterns or already known malicious instruction sequence. Anomaly based systems rely on trustful activity model with the use of machine learning and anything dissimilar from the model is alerted as suspicious. With the rise of IOT based environment use of such intrusion detection systems have grown multi fold.(**Elrawy, M., Awad, A. & Hamed, H**, **2018**) Intrusion detection systems can help in ensuring IT related regulatory compliance, maintain security standards, and raises alarms against malwares like spywares, keyloggers, unauthorized clients, unintentional accidental leakage etc., and measure the cyber-attacks in number and forms/types, increase efficacy. However, such detection systems are susceptible to few flaws like it has been witnessed that such systems often raise false alarms, unable to avid encrypted packets, they need to be continually updated and generally should be looked after by an expert engineer.

Strong Passwords, Firewalls, Encryption, Digital Signature, Clipper Chip, Routers/Gateways, Free software programs like security administrator tool, COPS, Omni Guard and Net probe which can identify any obstacle in the security mechanism and can be adopted to be safe at all times.

Check Your Progress 3 *Spend 3 Min*

Name any three cyber security software to fight against cyber-attacks?

1.5 CYBER SECURITY AND THE LAW

Cyber Law has played an instrumental role in regulating security issues and breaches in cyber space. Cyber law consists of Acts, Rules, Regulations, Notifications etc. passed by the Government of India. Information Technology Act 2000 is primary legislation governing cyber security in India. Besides, Government has also established Computer Emergency Response Team, Cyber and Information Security Division of Ministry of Home affairs, National Critical Information Infrastructure Protection Centre (NCIIPC), National Cyber Coordination Centre, National Cyber Security Coordinator, Defence Cyber Agency etc to ensure cyber security. Cyber security law is concerned with integrity, confidentiality, availability of public private information systems and seeks to protect individual rights like privacy, economic interests and national security.(**Jeff Kosseff, 2018**)

1. **Unauthorised access** - Unauthorised access is prohibited by law. As per Section 43 (a) of Information Technology Act 2000 (hereinafter IT Act 2000) makes any person liable for compensation if he is without permission of owner or any other person in charge of computer, computer system, computer network access or secures access. If the aforesaid act is done fraudulently or dishonestly then the person shall be liable for punishment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

2. **Distributed Denial of Service Attack** - As it is aimed to affect functioning of a website the act of carrying out Distributed Denial of Service attack shall disrupt computer network or computer system. It may also cause denial of access to persons who are authorised to access the said website. Aforesaid acts are prohibited by Section 43 (e) and (f) of IT Act 2000 respectively. Also, if denial of access attack is carried out with intent to threaten the unity, integrity, security or sovereignty of India or to striketerror in the people or any section of the people then the same shall be punishable under Section 66 (f) of IT Act 2000 with imprisonment for a term which may extend to imprisonment for life.

3. **Malwares** - Malwares like Botnets, Ransomwares, Trojan, Virus, Worms, Spywares etc. can be categorized as computer contaminants. Malwares are capable of modify, destroy, transmit data of programme residing in computer, computer network or computer system or usurp normal operation of the same, hence it is a contaminant as per Section 43 Explanation 1 (a). Malwares are capable of destruction, damage or adversely affect performance of a computer resource or capable of attaching itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource and hence includes computer virus as per Section 43 Explanation 1 (b) of IT Act 2000. Introduction of the malware leads to cyber contravention under Section 43(c)of IT Act 2000 and make the person who introduces it liable for damages by way of compensation. Similarly, if the introduction of computer contaminant or virus results in to destruction, deletion or alteration of information residing in computer resource or diminishes its value or utility or affects injuriously or steals, conceals, destroys or alters any computer source code used for computer resource with an intention to cause damage then it shall lead to

damages by way of contravention under section 43 (i) and (j)of IT Act 2000. If any of the aforesaid activities are carried out fraudulently or dishonestly then Section 66 of IT Act 2000 prescribes punishment of imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

4. **Social Engineering attacks** - These attacks harp upon psychological manipulation of victims and tricking the victim into revealing sensitive information. The victim is tricked to click on a malicious link or respond to fraudulent mail etc. Phishing - Its an activity by which the victim is deceived to reveal sensitive information like username, passwords, credit/debit card details etc by disguising oneself as a trustworthy entity. Coining of term Phishing is inspired from term fishing as in fishing, bait is cast to fool fishes similarly deceiving message/mail/webpage is cast to fool innocent.
As these attacks are carried out through impersonation, they are punishable under Section 415 of Indian Penal Code 1860. Also use of communication device or computer resource to cheat by personation is made punishable under Section 66D of IT Act 2000 is punishable with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees. Social engineering attacks are carried out to steal electronic signature, password or any other unique identification feature and hence the same is punishable under section 66C for identity theft which is punishable for a term which imprisonment of either description for a term which may extend to three years and shallalso be liable to fine which may extend to rupees one lakh.

5. **Cryptojacking** - It is unauthorised use of victims' devices to secretly mine cryptocurrency. Cryptojacking affects the functioning of devices as the same takes a toll on the device. Cryptocurrency is a virtual currency with no central regulatory or issuing authority and secured through cryptocurrency. Section 43 (a) and Section 66 of Information Technology Act 2000 prescribes compensation and imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both respectively.
6. **Exploiting vulnerability**- Vulnerability is a flaw in the measures taken to secure a device. Such flaw is exploited by the attacker to gain access over the device or harm it. Vulnerability is exploited and unauthorized access is secured. This is punishable under Section 43 (a) and Section 66 of IT Act 2000.

7. **Cyber physical attacks -** These are cyber-attacks breaching the security and impacting the physical environment. This may include shutting down of cameras, lights etc which are cyber controlled. Section 43 (d) and 66 of Information Technology Act 2000 prescribes penalty for causing damage and prescribes imprisonment if damage is caused with dishonest or fraudulent intention.

8. **IOT attacks** - Embedded devices that are connected to a network and capable of transferring data are at the risk of being attacked through exploiting vulnerability and can be hacked. Section 43 (a) of IT Act 2000 prescribes penalty for unsecured access and punishment under Section 66 of IT Act 2000.

9. **Web Jacking** - Webjacking a term inspired from hijacking, means when a website is hijacked or its access and control is taken over by the attacker. This is then misused for tricking the visitors of a website or defacement of a website etc. Section 43 (a) provides compensation for acts of unsecured access, Section 43 (d) and (e) penalises for causing

damage and disruption to computer network, computer system like what happen in defacement of website. Section 65 and Section 66 prescribes imprisonment and fine for unauthorised access and knowingly or intentionally conceal destroy or alter computer source code which generally happens during defacement of website.

10. **Drive by download** - A legitimate website is compromised and when the victim browses such a compromised website, the same installs malicious payload in the victim's device. Section 43 (c) prescribes compensation for introducing computer contaminant or virus and Section 65 of IT Act 2000 prescribes punishment for altering computer source code which may happen during drive by download attack. Besides, Information Technology Act 2000, Indian Penal Code 1860 is applicable to cyber offences, Trademarks law and Copyright law protects violation of Intellectual property in the form of domain names and software, Evidence law is helpful in prescribing the manner in which electronic evidence is admitted in the courts of law. There have been number of cases like altering of source code(Syed Asifuddin and Ors, 2005)Phishing,(NASSCOM case, 2005)data theft(Gagan Harsh Sharma case, 2019), hacking(M/S.Sundaramcase, 2011)etc. where courts of law have punished offenders guilty of breaching cyber security.

Selected Case Laws

1. In Pune Citibank MphasiS Call Center Fraud(**Malini Bhupta,2005),**employees of a Company cheated US customers of Citibank. The fraud involved securing unauthorized access to computer system which was punishable under Section 43 and 66 of Information Technology Act 2000.
2. In Syed Asifuddin and Ors. v. The State of Andhra Pradesh,2005, It was alleged that employees of a company manipulated electronic 32-bit number (ESN) programmed into Samsung N191 and LG-2030 cell phone instrument. This amounted to alteration of computer source code and the act was punishable under Section 65 of Information Technology Act 2000.
3. 26/11 Terror attack investigation revealed that terrorists hacked systems to access data with computer systems of hotels which were under attack. The attack squarely fell under Section 66F of Information Technology Act 2000**(Ilardi, Gaetano,2009)**
4. Abhinav Gupta v. State of Haryana, 2008, highlights that Stealing and sharing of confidential/copyright material falls within the ambit of Section 66 of IT Act 2000 and hence punishable.

1.6 SUMMARY

Challenges to cyber security exists in the form of unauthorized access, exploiting vulnerability, cyber physical attacks, IOT attacks, Web jacking, drive by download, crypto jacking, social engineering attack, malwares, denial of service attacks etc. These may be prevented with the help of technologies, practices and remaining vigilant. Few of the most common technologies or practices are updated firewalls, strong passwords, patching operating systems, two factor authentications, etc. which can help in preventing cyber security attacks. Law also acts as a deterrent factor for those who attack cyber security. Law prescribes punishment in the form of fine, imprisonment etc. for cyber law violations. Cyber

security attacks may also cause intellectual property violations and hence attract law regulating the same. An information technology law empowers enforcement agencies with investigative powers and recognizes electronic evidence admissible in the courts of law. However, threat to cyber security in the form of cyber-attack can be carried out anywhere in the World and hence for enforcement of cyber security law and bring culprits to justice it's necessary that all the States come together and collectively fight against those who pose threat to cyber security.

1.7 Solution and Answer

Check Your Progress

1 Benefits of Digital Security are:-
   a. Protection of Data
   b. Prevent unauthorized access
   c. Prevent cyber attack
   d. Builds trust in the integrity of online communication or transaction.

2 Phishing is an activity by which the victim is deceived to reveal sensitive information like username, passwords, credit/debit card details etc by disguising oneself as a trustworthy entity.Yes, it is threat to digital security.

3 Firewall, Firmware, Network intrusion detection software etc.

1.8 REFERENCES AND FURTHER READINGS

- Abhinav Gupta v. State of Haryana (2008 Cr LJ 4536)
- Andrew Murray(2013). *Information Technology Law: The Law and Society*. 2nd ed: Oxford University Press.UK
- Chizari, Hassan &Zulkurnain, Ahmad &Hamidy, Ahmad & Husain, Affandi. (2015). Social Engineering Attack Mitigation. *International Journal of Mathematics and Computational Science.* 1. 188-198.
- Dr S.R. Myneni. *Information Technology Laws*. First Edition.p497-519
- Elrawy, M., Awad, A. & Hamed, H (2018). Intrusion detection systems for IoT-based smart environments: a survey. *J Cloud Comp 7, 21. Retrieved from* https://doi.org/10.1186/s13677-018-0123-6.
- Gagan Harsh Sharma v. The State of Maharashtra 2019 CriLJ 1398
- GOsafeonline (2014).Denial of Service.Singpore Government Website Agency.Retrievdon 12/09/2020 from https://www.csa.gov.sg.
- Ilardi, Gaetano. (2009). The 9/11 Attacks—A Study of Al Qaeda's Use of Intelligence and Counterintelligence. *Studies in Conflict & Terrorism* - STUD CONFL TERROR. 32. 171-187. 10.1080/10576100802670803.
- Information Technology Act, 2000. Retrieved from https://www.indiacode.nic.in/.
- Jeff Kosseff (2018). Defining Cyber security Law.*103 Iowa L. Rev. 985*

- M/S.SundaramB.N.P.ParibasHome v. State of Tamil Nadu W.P.Nos.2513 of 2011.
- Malini Bhupta(2005). Pune call centre fraud rattles India's booming BPO sector, raises questions on security. Retrieved from https://www.indiatoday.in/magazine/economy/story/20050502
- Mark Burnette (2020). Three Tenets of Information Security. Retrieved from https://www.lbmc.com/blog/three-tenets-of-information-security/
- Micheal Nadeau (2021). 'What is crypto jacking? How to prevent detects and recovers from it'. Retrieved from https://www.csoonline.com/.
- Ministry of Electronics and Information Technology Notification (2018). Retrieved https://www.meity.gov.in/writereaddata/files/NCIIPC-Rules-notification.pdf
- NASSCOM v. Ajay Sood 119 (2005) DLT 596
- OECD (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264245471-en
- Paul Todd (2015). *E-Commerce Law*. Taylor and Francis Publications.
- Sharma Vakul (2019). *Information Technology Law and Practice- Cyber Laws and Laws Relating to E-Commerce*. 6th Edition, LexisNexis, Haryana
- Singh Talwant, (2011). *Cyber Law & Information Technology*. New Delhi, India.
- Singh Yatinder Justice (2016). Cyber Law. 6th ed. Universal Law Publishing Co.India
- Steve Hedley and Tanya Aplin (Ed.) (2008). *Blackstone's Statutes on IT and e-commerce* 4th edition: Oxford.
- Syed Asifuddin and Ors. v The State of Andhra Pradesh And Anr. 2005 Cri LJ 4314.