Law Journals
A Treasure Trove of Legal Knowledge.

National Journal of Cyber Security Law
Volume 1, Issue 1
www.stmjournals.com

Cybersecurity: Techno-legal Domains

M.K. Nagaraja*
Visiting Professor of Law, KLE Law College, Bengaluru, Karnataka, India

Abstract

In the information age or the digital era, cybersecurity measures require the adoption of international standards by scrupulously complying the international protocols and norms since the digital assets of a corporate company or organization and intangible property under the intellectual property regime have assumed money value as what William Gibson predicted three decades ago. The cybersecurity comprises of both physical and logical security, implying the system hardening and layering security measures in tune with the cybersecurity policy. Information processed by the corporate company needs to be protected and secured by the top-level management on a high priority basis by providing the required resources in a cost-effective manner. All the risk factors, threats and vulnerabilities should be analysed, processed and complied by affording technological and legal safeguards. The plans, approaches and strategies should be formulated by the top level management to mitigate and provide solutions to the challenges posed by the cyber attackers. Cybersecurity being the long-term strategy for high structured corporate Companies, the security 'programme document' is required to be prepared and reviewed periodically. The top security sleuths should exercise due diligence to confine to the 'business specific' needs than resorting to 'overstepping details' in the security document to avoid confusion. The latest trends of attacks should invariably be addressed in a copious manner towards achieving the goals and objectives of an organization. In order that the security plan to be successful, the responsibility should start with the top level management and made functional at every single level with the 'need to know and need to do basis.

Keywords: *Cybersecurity, security trends, risks, attacks, Botnet, Attack Vectors, threats, vulnerabilities, system hardening, layering security, security policy, processes, review, controls, digital forensics, digital assets, proprietary assets, role-players, responsibilities, mitigation, remediation, training, techno-legal solutions*

**Author for Correspondence* E-mail: drmknagaraja@gmail.com

CYBERSECURITY IN PERPETUITY

Conspicuously, cybersecurity is a perennial issue than a static one for the simple reason that the new forms of cyber attacks emerge with the growth and development of technologies or convergence of such technologies. Cyber attacks imply all types of computer or Internet-related technology driven cyber attacks. What is protected today may be obsolete tomorrow owning to the technological progress of different technologies like; ICT [1] and IWT [2]. The convergence of ICT and IWT has enhanced the scope of information security in as much as sharing of such information in the business pursuit. It is incumbent that the cybersecurity experts need to upgrade their skills, knowledge and abilities to cope with the new form of cyber attacks. From the viewpoint of business economy, the cybersecurity implies protection to the digital assets as well as proprietary assets, while in the viewpoint of technology, it implies securing of the computer system and the network against internal and external attacks. The coordinated efforts of cybersecurity experts, managers, consultants and forensic experts are absolutely essential to fully secure the computer system, network, digital or proprietary asset in the virtual environment. Jon Oltsit, an Information Security System Association felt that the deficiencies in cybersecurity skills and expertise lead to existential threats. Even the research conducted by the two research agencies like; the CSG [3] and ISSA [4] made their cogent observations that the deficiency in the skills of cybersecurity shall be supplemented by the advanced skills in areas of cybersecurity analysis, forensic analysis and cloud computing security. In this perspective,

on-going training for the cybersecurity sleuths on all crucial issues is the need of the hour towards combating the new form of threats, risks and vulnerabilities [5], which I shall be discussing in this article a little later.

SIGNIFICANCE OF INFORMATION

William Gibson, in his science fiction titled; "Neuromancer" (1984) said that "information is money and nothing but money in the near future." Within a decade of time, his prediction proved to be true. In the present information age, the processed information forms the digital asset of a high structured corporate Company or organization. It should be viewed that intellectual property or proprietary assets forms the capital for many MNCs [6] and TNCs [7] in the global economy. The digital assets of the processed information are of greater significance to the business entities in the LPG [8] scenario. There is dire need for protecting such digital or proprietary assets that are stored in electronic form in the virtual cyberspace. With the increased interconnectivity comprising of different manifestations of the Internet, the digital and proprietary assets are exposed to threats, risks and vulnerabilities, the OECD [9] issued guidelines on information security systems and networks since the intangible property is stored in electronic form which moves electronically. The cybersecurity should cover a set of suitable security policy, organizational structure, procedures, processes and controls. Access control assumes tremendous significance in as much as defining the role of each employee and the extent of his accessibility on a 'need to know and need to do basis'. It is all the more necessary for the cybersecurity experts to implement, monitor and review security measures periodically. The security controls can be achieved by technical and legal means, before which the security needs should be identified. The statutory and regulatory mechanism assumes significance in the perspective of the risk management. The outcome of the risk assessment forms the guiding principle for the management to work out the priorities to secure the computer system, network, digital assets and intangible assets in the electronic realm. Of course, the real task arises for protecting the digital data in the absence of Data Protection Act in India [10]. Even the Personal Information Protection Bill, introduced in the Parliament in 2006 is yet to see the light of the day. Software piracy is going spree in the absence of adoption of 'Zero Piracy Policy' by the Government of India. In the absence of such legal safeguards to protect against cyber attacks, the critical infrastructure can hardly be protected. The story of success much depends on the technical safeguards than the legal safeguards. The plethora of cyber attacks like; the data-related attacks [11], software-related attacks [12] and technology-related attacks [13] inclusive of attacks on websites, e-mail attacks and newsgroup attacks that are producing adverse effect on the cybersecurity.

MASTER PLAN

The Cybersecurity Management System (CMS) is briefly depicted in the diagram given below:-

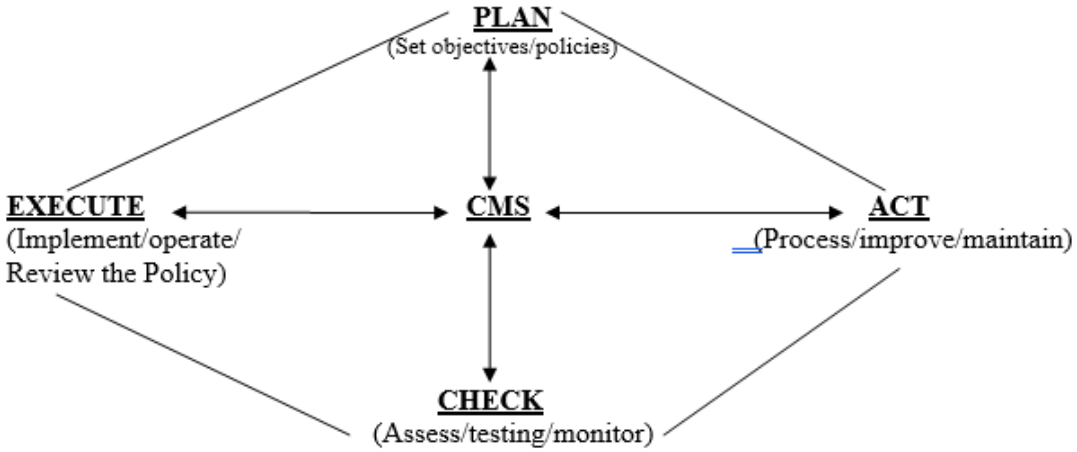

Fig. 1: Cybersecurity Management System

Cybersecurity affords protection to the systemic infrastructure, digital assets, intellectual property rights, trade secrets and verbal and visual communications. It also protects against the nation-sponsored attacks and Advance Persistent Threats. The layering defence or defence in depth is an essential factor of the cybersecurity for tracking the cyber attacks. The composition of cybersecurity shall include cybersecurity experts, architects, consultants, digital forensic experts, top level managers and network specialists. It is incumbent that all cybersecurity domains shall be addressed in a more effective manner to ensure foolproof security. All the three approaches for namely; international standards, risk-based and compliance-based security approaches are essential for the implementation of cybersecurity measures. The main focus of cybersecurity is designing, implementing, controlling and managing.

TRENDS

Before understanding the cybersecurity dimensions or its intricacies, it is absolutely necessary to comprehend fully the 'security evolving technologies' to effectively combat the new forms of attacks. "A proper understanding of the intrusive tools availed by the attackers in the present millennium gives an insight into the cybersecurity risks and threats." The cybersecurity experts should be fully aware of the common patterns of attacks. It is incumbent to realise that new cyber attacks in different forms like; Botnet [14], Botnet is capable of hijacking 1300 Internet accessible video cameras enlisting them as pawns [15] in 4000bps DDOS attacks targeting the Banks and Gaming firms. The cyber perpetrators behind the Botnet start phishing out million e-mail messages a day. The notorious Necurs Botnet [16] is capable of spewing [17] huge volumes of e-mail containing improved version of Potent Locky Ransomware and the Dridex Banking Trojan. Attack Vectors [18]. Rootkit is also a malware that hides other malwares by modifying the Operating System (OS) software of the computer and poses external and internal threats to the cybersecurity. FlokiBot, a new financial malware based on 'zeus 2.0.8.9' source code [19] is specific to the attacks on Banking and Insurance Companies is clandestinely sold in the Dark Web Market or Dark Net Market to grab 'point of sale' (POS) data via the aggressive Spear Phishing and RIG Exploit Kit by inserting the malicious code called the "Explorer exe" as a hooking method to track the crucial data from the memory. The 'spear phishing' attack makes it appear as though it has originated from inside of an organization and such attacks are directed against governments, defence organizations and scientific or research institutions. In 2013, zeus code was used for constructing a 'citadel malware' to steal banking and financial information. Cyber attackers resort to Object Linking and Embedding (OLE) technology to spread malware by placing malicious code in the OLE Code in a formatted text or digital images. A document in OLE enables word processor to accept an embedded spreadsheet. LizzardStresser Internet of Things (IOT) Attack Vectors form the significant threats so far as clients are concerned as they target the recipients. The ingress (intrusive) and egress (exfiltration) Attack Vectors are resorted by the attackers to remove the data from the computer system and the network by exploiting the vulnerabilities. Phishing attacks are also directed against the recipients who have an access to the protected information system as it gives an impression to the user that the originator is a genuine person. The cyber attackers avail the malicious code or a software as malware to gain access to the targeted computer system with an intention to disrupt the computer operations or to steal the classified [20] information. The malware software tool is used for cyber espionage or 'skywiper' which is capable of tracking the keyboard, network traffic, screenshots, audio-video communications. Spyware is a malware category that gathers information about an individual or organization. Ransomware is a malware used for extortion of payment that encrypts and decrypts the data. Key logger is a malware that secretly records user keystrokes and the screen content. The 'kill' command wipes out the traces of malware from the computer system. Stuxnet [21], a computer worm highlights the malware's potential to disrupt adversary control, data acquisition and the programmable logic controllers used in

power plants. Trojan is a malware with which access is gained to a targeted computer system by hiding the real application. Network worm is a self-replicating code designed to spread across the networked computers. Advanced Persistent Threats (PPTs) are robust and complex threats directed against the corporate entities. Backdoor gains access into the compromised computer system by installing the software to gain remote access. Blackshade, a malware allows tracking passwords, information, images and online accounts or documents. The Brute force attack is a combination permutation to decipher the correct passwords and encrypted keys. Buffer overflow is a security attack on the data integrity as it contains codes. XSS Attacks or cross-site scripting by which a malicious script-code are injected by using web application. Man-in-middle attack is carried out to gain control over communication stream between the two-ends of the victim system. The cyberpunks who monitor the movement of packets in the cyberspace and intercept the communication of banking or financial data in order to perpetrate online frauds in the Online Fund Transfer (ORT) or Electronic Fund Transfer (EFT). The attackers adopt the 'pocket sniffing' method by inserting the software program from a remote network location or host computer to monitor information packets sent from the Company's computer system and obtain password of a legitimate user by masquerading technique to gain access. By resorting to the 'site cloning' method, the customers of banks and financial institutions are lured to reveal their smart card information to a fake or forged website. The false 'merchant site shops' are set up by the perpetrators with an intention of stealing the smart card information on the pretext of offering services. The cyberpunks keep track of the movement of packets travelling in the cyberspace and perpetrate online frauds by diverting the fraction e-money to their fraudulent accounts. Vladimir Levin, a Russian has committed theft of digital money and transferred to his 40 illegal accounts. Sometimes, information is retrieved from the 'digital dumps', 'files constellation', 'digital constellation', trash or printer buffers due to unsecure computer system. The Mobile malware is an emerging threat in the cyberspace. I can recall the U.S. Government adopting 'Zero Tolerance' to cyber terrorism in order to fully secure the networking system. The key considerations for digital forensics lies in auditing the network devices, configuring mission-critical application for performing security auditing, maintaining the database, file hashing and checking the integrity. Now-a-days, increased connectivity ensured through mobile devices, cloud computing infrastructure, third party relationship, information sharing agreements and automated business processes are prone to cybersecurity risks.

CORE TASKS

The core task of the cybersecurity is to (a) to identify the problem, (b) to put in place the Incident Response Team (IRT), and (c) to effectively manage the cybersecurity risk factors of a network system. It must be realized that securing the 'digital asset' and internal or external intrusions of an organization against attacks is the need of the hour. Such cyber attacks could be of 'common attack patterns' or 'unforeseen attacks'. A copious study and research is all the more necessary to comprehend fully the 'common attack patterns' which may include Brute Force, Spear Phishing, Masquerading[Masquerading means spoofing or shoulder surfing technique], Cross Site Scripting, Backdoor, Buffer Overflow, SQL injection[Secure Query Language] and Zero-day Exploit attacks. Information security compliance being the utmost priority the security needs, it should be more of compliance-cum-action oriented. The top level management should seek the services of the cybersecurity experts, auditors, technical and legal experts as a coordinated effort. It must be realized that security programme being a long-term strategy, it should be realistic in tune with the policies, programmes and strategies to match the real-time situation challenges. Basically, the cybersecurity involves; (a) system hardening, (b) layering security, and (c) protection of digital assets. The system hardening is the process of implementing security controls on a computer system with perfect access control. Unless the system hardening is ensured, risks, vulnerabilities and threats are bound to persist owing to the risk of exposing the computer system. In the 'system centric', emphasis is laid on the controls at the

system level to protect the digital assets or information stored therein, while in the 'data centric', emphasis is on the protection of electronic data regardless of its location. To achieve better layering security, the 'defence in depth' is a felt necessity towards formulating external cybersecurity strategies by implementing multiple control layers for preventing and detecting external attacks. The horizontal defence in depth controls are placed at different locations in the path of access, while the vertical defence in depth controls are placed at different levels of the system layers like; the hardware, application, OS and database. The Internet technology has expanded new vistas for 'perimeter security'. Owing to outsourcing, mobile computing or use of mobile devices and host services need to be secured. The perimeter becomes the 'line in defence' to protect an enterprise against external threats by monitoring the network ports, hubs, gateways, route traffic and private virtual network (VPN) traffic. VPNs can be designed in such a way so as to ensure to carry out all types of electronic data in a secured manner. The Transmission Control Protocol (TCP) provided reliable and sequenced error-checking method. TCP/IP uses the web protocol, hypertext transfer protocol [http] and port at the higher level applications of pre-assigned by the Internet Assigned Numbers Authority (IANA). The cybersecurity experts should also realize the need for Operating System (OS) security towards protecting the critical information. The layering security relates to the perimeter security by installing the firewalls [22] against external attacks. Firewalls provide layered protection to information or digital assets of an organization. The 'screened-host firewall' provides the layer and application servers security, while the 'dual-homed firewall' filters all traffic passing through the network. All the seven layers shall be secured since each one of the layer performs its own function. The physical layer manages the signals of the network system with repeaters, while the network layer translates the network addresses and the route of electronic data from origin point to destination point. If the data link layer divides data into packets for being transmitted, the transport layer ensures reliability of the data transmission in a proper sequence. The sessions layer coordinates the user connections and the presentation layer formats the data. Finally, the application layer moderates the application software with the network services. Both piggybacking and eavesdropping techniques are adopted by the attackers to circumvent the network controls to carry out cyber attacks. The cybersecurity threats [23] may arise on account of internal or external attacks. Such attacks may disrupt the business activity of an organization or a corporate company steal the financial information [smart card numbers of the customers of banks are cloned or counterfeited for the purpose of purchasing merchandise products in the Tele-market], proprietary data of Intellectual Property Rights' holders. Spyware or Skywiper [24] for espionage activities. The vulnerability of threats by way of 'residual risk' persists due to the outdated cybersecurity architecture and non-adoption of security controls and strategies even after the mitigation and remediation. The third party data management being the cloud-based services, it involves the risk of plagiarism, misuse or alteration of data which requires protection. The threats are either 'adversarial threat event' or 'non-adversarial threat event'. The former is done by the human agent as an adversary and the latter due to mishandling of critical information by the unauthorised users, incorrect privilege settings, natural calamities at the corporate office, insertion of vulnerabilities into software products (like; Trojans, viruses or maintenance hooks) and obsolete equipment or formatted disk. Though online threats are invisible, they are real in nature.

THE POLICY

Cybersecurity policy is the primary task of the security governance by the management since it specifies the security needs and defines the roles and responsibilities in a given organization. The policy should be properly formulated and validated before being implemented. It is essential that the cybersecurity policy and cybersecurity laws should be in consonance with each other. In other words, the policy must facilitate the law for proper implementation and laws should support the policy in its real sense. In the event of contradictions between the policy matters and the legal matters, it will end up in a fiasco.

Cybersecurity being ever-changing, it requires continuous monitoring, updating, testing and changing in tune with the growth of cyber technologies. The ability to integrate business processes and technology is significant since it links the people to the system and authentication or authorization [25] services of an enterprise. The security architecture describes the structure, components, connections and layouts of the security controls. The attributes of a good policy lies in the articulation of well-defined cybersecurity strategies and compliance measures with expectations from the role-players. The small organizations may adopt 'effective practices' instead of formulating the security policy. The primary object of the cybersecurity policy should be the commitment and support of business requirements and implementation of the cyber laws, regulations and the technological measures. The top management of an organization must approve the 'policy document' before publishing or communicating it to the concerned including the employees. It must clearly specify the business objectives and strategies inclusive of the standards [26] of compliance requirements, training and advocacy and the consequences of violation of the policy. It is essential that the cybersecurity policy needs to be reviewed periodically and effect changes wherever it is felt necessary. Such changes may relate to the creation of additional infrastructure, regulatory measures, technical measures and updating the obsolete system only after analysing the new trends arising out of the risk factors, vulnerabilities and threats. The policy should be revised by incorporating 'improved measures' with the approval of the top management. The Government of India adopted the National Cyber Security Policy (NCSP) through the Department of Electronics and Information Technology on July 2, 2013 [27] in response to the National Daily Newspaper publishing the documents leaked by the National Security Agency (NSA) whistleblower Mr. Edward Snowden. The key concept of the policy lies in its confidentiality, integrity and availability. Adoption of sister technologies like; Cryptography and steganography inclusive of digital signature ensures integrity and confidentiality. The Policy provides for (a) securing and safeguarding the public and private infrastructure against cyber attacks, banking and financial information and the sovereign data information of the nation, and (b) building resilient cyberspace [28] for the citizens, businessmen and the government. The policy stipulates 'Ten Command Lines' inclusive of the circumventing the resultant instability due to cyber attacks, setting up of the National Critical Infrastructure Protection Centre (NCIIP) to effectively address all forms of cyber threats to the Information Communication Technology (ICT) as part of crisis management, designating the Computer Emergency Response Team (CERT) as nodal agency for cyber security-related issues, creating the task force comprising of cybersecurity professionals for capacity building or skill development or imparting training, encouraging the information security professionals to establish cyber security laboratories, encouraging the Public key Infrastructure (PKI) for government services, etc. "The most significant provision of the National Cyber Security Policy, 2013 lies in the provision for development of a 'legal framework' and technological safeguards to meet the cybersecurity challenges." Glaringly, the policy is silent about the need for enactment of Cyber Security Law for the country or made any reference to the Information Technology Act, 2000 [29]. "The cybersecurity laws of India must be crystal clear so as to reflect the National Cyber Security Policy." Symbolically, if cybersecurity laws are the eyes, policy shall be the heart; eyes being the windows of the heart and windows implying effective implementation of laws. At present, there is no Cyber Security Act enacted in India. A pertinent question arises in the minds of the legal luminaries as to which law governs the National Cyber Security Policy? At least, the Government of India could have issued a Notification stating that the Information Technology Act, 2000 is applicable to the cybersecurity issues and challenges with suitable amendments to the Act. The matter needs to be reviewed by the Law Commission of India (LCI). Following are a few suggestions for the LCI in the implementation of Cybersecurity Policy:-

- Developing cybersecurity risk-management strategy in tune with the

policy, procedures, standards, baselines and guidelines.

- Listing the cybersecurity risks by the risk analysis and evaluation to determine the estimated risks and events for compliance.
- Creating I.T. security Standard Operating Procedures (SOPs) as the code of practice for cybersecurity sleuths.
- Setting the Benchmark of cybersecurity by adopting ISO 19011: 2000 standards.
- Adopting the cybersecurity 'Master Plan' and the 'program document'.
- Constituting, commanding and controlling the Incident Response Team.
- Monitoring the implemented cybersecurity measures by adopting the 'performance metrics'.
- Adopting the 'cybersecurity advocacy' for creating awareness on cybersecurity-related issues and imparting training among the sleuths of Incident Response Team as part of familiarizing the cybersecurity concerns among the 'role-players'.
- Reviewing the mitigation measures and the non-compliance measures for remediation.
- Implementing the methods, approaches and processes of cybersecurity auditing as an offering of both physical and logical security cover against attacks by specifying clearly the role of cybersecurity experts and their responsibilities towards evolving and initiating strategies in the task of mitigating the risks and threats and to implement multiple control layers periodically as part of remediation.
- Performing the Security Impact Analysis (SIA) by the top management and the team-experts, constituted for the purpose.
- Documenting the lessons learnt based on the feedback received from the team-experts.
- Offering legal services inclusive of other related legal issues likely to be taken up before the Cybersecurity Tribunals within the ambit of the cybersecurity policy.
- Developing the digital forensics to deal with the real-time challenges.

TECHNO-LEGAL DOMAINS

As far as techno-legal domains of the cybersecurity are concerned, it is amply evident that the technological safeguards adopted by an organization or a corporate Company are more or less adequate to a specific challenge to protect the computer system or networks and the digital asset or intangible movable property in the virtual environment. The real question that arises in the minds of the cybersecurity experts or consultants is about adequacy of cyber laws, rules and regulations in India when compared to advanced countries of the world. The Personal Data Protection Act (PDPA) governs the data collection, its use, disclosure and the rights of the owner of personal information. The Personal Data Protection Commission was constituted on January 2, 2013 to enforce the Act. Internationally accepted protocols requires that the personal information should be processed before disclosing it to the third party with the consent of original owner and such information cannot be further processed which is incompatible with the purpose for which it is already processed. In April 1985, the Organization for OECD issued guidelines on privacy and trans-border flows of personal information. In 1990, the European Union (EU) also issued guidelines on the protection of personal information. The United Nation Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce, 1996 defines the 'Data Message' as "information generated, sent, received or stored by electronic, optical or similar means including, but not limited to electronic data interchange, e-mail, telegram, telex or telephony." The Model Law also assures the 'functional-equivalence-approach' to both physical and virtual information. Further, Article 5 of the Model Law mandates that information shall not be denied legal effect, validity or enforceability on the ground that information is in the form of data message. Article 2(f)) of the Model Law defines the 'Information System' as "a system for generating, sending, receiving, storing or otherwise processing the data message." Section 2(r) of the Information Technology Act, 2000 defines an electronic record as "any data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computers generated micro fiche." It is incumbent to realize that an electronic document comprises of the text (data), graphics (picture form), voice (Voice

over Internet Protocol), Audio-Video and computer program (software). A database containing printable information qualifies for information. Information having commercial or intrinsic value is regarded as intangible property as observed by Justice Houlden of the Supreme Court of Canada in R v. Stuart that, "while clearly not all information is property, I see no reason why confidential information which has been gathered through the expenditure of time, effort and money by a commercial enterprise for the purpose of business should not be regarded as property and protected under criminal law." The Scottish Law Commission in the Working Paper on Conspiracy to Defraud observed, "Confidential information could be regarded as valuable commodity as it is frequently bought and sold." Therefore, the 'digital asset' or 'proprietary asset' is a valuable commodity for a corporate Company or an organization. The 'property status' to information or intangible property was assured by the European Commission (EC) by its Directive No. 84/374. European Conventions held in 2001, 2003 and 2005 listed the protocols on privacy of communication and protection of information. "Information occupies the prime place in the entire global economic activity in the neo-economic order as it is fundamental to the business activity." In India, there is no Data Protection Act unlike in the United Kingdom and other countries of the world. The Personal Data Protection Bill of 2006 introduced in the Parliament has since been lapsed. Section 72 of the Information Technology Act, 2000 prescribes punishment up to 2 years imprisonment or with fine which may extend to Rs.1 Lakh, or with both for securing access to private information without the consent of its original owner and disclosing the same to the third party. Information, whether it is private, price sensitive and confidential cannot be shared unauthorisedly. However, the policy made no mention bout the I.T. Act. The sensitive data including the financial information, health information or medical history records, sexually orientated information and biometric information requires to be protected against unauthorised use. In Japan, a computer engineer was arrested for stealing information of 29,000 clients of Sukura Bank in Tokyo and selling it for 200.000 Yen.

CONCLUSION

To conclude, the security risks are posed to the digital assets, local area network (LAN), wide area network (WAN) or wireless local area network (WLAN) [30]. WLAN connects computers and other components to the network using an access point device called the "wireless networking hub" with a malafide intention of carrying out cyber attacks. WLAN technologies conform to varying levels of security features. Implementation of prioritized security controls on the basis of the magnitude of risks and threats is advisable for the cybersecurity experts. Consequent to the risk assessment, risk analysis and risk evaluation, the risk mitigation and remediation plans needs to be adopted. Intrusion Prevention System (IPS) predicts an attack before it occurs and prevents malicious programs. The Control Objectives for Information and related Technology (Cobit) is a model framework for I.T. governance which defines the goals and controls for the business needs and it addresses how to plan and organize, acquire and implement, deliver and support and monitor and evaluate. It also lays down the complete roadmap to the framework and control objectives, apart from providing a set of information security policy like; the risk management, asset management, vector management and disaster recovery.

REFERENCES

1. Abbreviated as 'Information Communication Technology' which gave rise to cyber crimes
2. Abbreviated as 'Internet Wireless Technology' resulting in the emergence of Voice Over Internet Protocol (VOIP) crimes
3. Abbreviated as Computer Systems Group, a global digital leader.
4. Abbreviated as Information System Security Association.
5. Vulnerabilities are of imminent danger to cybersecurity.
6. Abbreviated as Multi-National Companies.
7. Abbreviated as Trans-National Companies
8. Abbreviated as Liberalization, Privatization and Globalization.
9. Abbreviated as Organization for Economic Cooperation & Development

10. The Shere Committee (1995), constituted under the chairmanship of Mrs. K.S Shere recommended for enactment of the Data Protection Act as a long-term measure, but in vain.
11. The data-related cyber attacks mainly include plagiarism or data theft, data diddling, masquerading or shoulder surfing, phishing and criminal damage to data etc.
12. Software-related cyber attacks include software piracy, source code theft, packet sniffing, cloning of smart cards, online frauds etc.
13. Technology-related cyber attacks include hacking, cracking, whacking, piggybacking, eavesdropping, spiking, distributed denial of services (DDOS), cyber terrorism etc.
14. Botnet is an automated robot distributed across the compromised computer network to launch Denial of Service attacks.
15. The pawn has no real power but controlled and used by others to achieve some result to their advantage.
16. Necurs is the largest Botnet with 6.1 Bots capable of causing loss of millions of dollars which was developed in July 2016.
17. Spewing implies ejecting large volumes of e-mail data by force.
18. AttackVectors could be ingress (intrusion) and egress (exfiltration) vectors, wherein the former launches the attack on moving data in the cyberspace and the latter circumvents the network controls to gain ingress into the computer system or the network.
19. This source code is a Trojan that surfaces at a later stage.
20. A website contains huge information which is of general nature, classified or unclassified data and the classified information comprises confidential or price sensitive data.
21. Stucknet was discovered in 2010.
22. A firewall includes packet filtering, application firewall systems, dynamic packet filtering tracks and next generation firewall.
23. Threats imply the potentially hostile activity by the cyber attackers in the internal or external environment.
24. Skywiper was discovered in 2012.25. A Authorization implies the 'need to know and need to do basis'.
25. Authorization implies the 'need to know and need to do basis'.
26. Standards imply the mandatory international norms or protocols which provide the means to specific application and procedure; International Organization for Standardization (ISO) and International Electro-technical Commission (IEC) together with the Joint Technical Committee have developed international standards in the field of information technology.
27. http://appknox.com/aglance-at-medias-cybersecurity-laws/
28. The term 'resilient' is derived from the Latin word 'resilire', meaning 'to spring back to the shape' or able to quickly return to the good condition.
29. This Act was amended in 2008 with effect from 2009.
30. WLAN connects computers and other components to the network using an access point device called the "wireless networking hub" with a malafide intention of carrying out cyber attacks.

Cite this Article
M.K. Nagaraja. Cybersecurity: Techno-legal Domains. *National Journal of Cyber Security Law*. 2018; 1(1): 56-64p.