IMPLEMENTATION OF CYBER SECURITY MEASURES FOR ROAD READY DRIVERLESS CARS OF BUSINESS HOUSES

Written by ***Dr. Rajlakshmi Pushkaraj Wagh***

B.Com, NIIT, LLM, PhD (Law)

Abstract:

The paper anchors on the implementation of cyber security measures in business organization. There is an Endeavour made by the author to bring out the model policy adopted by business organization in order to safe guard their confidential information from hackers and cyber criminals. Cybercrimes are motivated by socioeconomic, psychological and geopolitical factors.[i] Tough the Indian Legislation plays an important role in safe guarding the vulnerable data of the corporate yet there is a need for business organization to frame in-house policy for the protection of their confidential information and to have a more comprehensive protection against adversaries. This paper would through light on the measures required to protect one from internal and external attackers and defenses that adapt quickly from threats.

Keywords: Malicious, Cyber Security, spyware

Introduction:

In the era of digitalization many business houses are taking prominent role in digitalization and transforming data into bytes. There is a move towards a more environmental friendly office work. Business houses are inclined towards a paperless office. Most of the data are stored in Cd's /pen drives/ internet. Today the data is accessible from any part of the world. This has given rise to different types of cybercrimes. Today hackers are rendering part of internet as unreachable. A crime adopted by them to

create ripples in big business houses. The Denial-of-service attack is an oldest form of attack which paralyses the users in accessing websites[ii]. Accurate and crucial data is required for business organizations and preventions of such are a must. Though there are cyber security package available in the market yet there is a need for in- house policies. The malicious employees may leave no stone unturned to harm the organization. There is a single lone legislation i.e. the Information Technology Act, 2000, in India, which governs the internet.

Cyber Laws in India:

Even the inventors of Internet could not have really anticipated the scope and far reaching consequences of cyberspace. The growth rate of cyberspace has been enormous. Internet is growing rapidly. With the population of Internet doubling roughly every 100 days, Cyberspace is becoming the new preferred environment of the world. Since 1999 till date the number of internet users has increased by ten folds.[iii] With the spontaneous and almost phenomenal growth of cyberspace, new and ticklish issues relating to various legal aspects of cyberspace are cropping up. In response to the absolutely complex and newly emerging legal issues relating to cyberspace, CYBER LAW or the law of Internet came into being.

The Information Technology Act,2000 provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 .[iv]

Cybercrimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code.

The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000. Cyber law is a much newer phenomenon having emerged much after the onset of Internet. Internet growth is completely unplanned and unregulated. Billion Dollars are spent on creating and maintaining brands in the corporate worlds which is revenue to the company.[v] There is a need to have Fast Track courts to settle cybercrime cases. [vi] Cyber-crimes are always a threat. These are in all shapes and sizes and target big business houses.

Cyber Security Issues in India

- **Centre of Excellence & Internet of Things in India**[vii]: IoT can be used for smart grids, smart cities, e-health, etc and thereby reduce their cost of operation and improve their productivity. They are multi – industry platforms that support anything. However, IoT also has civil liberties and cyber security challenges to manage. Cyber criminals have already started abusing IoT controlled devices for launching malicious cyber-attacks. As the technology protocols for IoT are still evolving, it is very difficult to avoid such cyber-attacks. Today the whole globe has been converted into an e-market place. Similarly, on the legal framework front, IoT has yet to be suitably regulated around the world. India has no dedicated law for IoT though some guidance can be found from the Information Technology Act, 2000.

  Mobile Cyber Security in India: The big scale use of mobiles also give rise to cyber law and cyber security issues that Indian government must be well prepared to deal with in future. Mobile phones have become ubiquitous these days. They are used for multiple purposes ranging from personal use to mobile banking. Cyber criminals have also realized the importance of mobile phones for committing cybercrimes and financial frauds. In the case of *State vs. Mohd. Afzal* [viii]

the police confiscated mobile phones and other electronic gadgets, which were used to commit the terrorist attack. Further the question arose whether computer print outs were admissible as evidence.

- **Health Care Cyber Security Issues**: Healthcare industry is facing diverse range of cyber attacks these days. The prominent among them is ransom war that encrypts the sensitive healthcare information and decrypts the same only once the ransom is paid. Presently, healthcare cyber security market consists of protection against malware, DDOS, advanced persistent threat, spyware, lost and stolen devices, etc. The health care sector is facing issues like misuse of personal health information. These systems may be taken as unsafe by people. Most of the communication in health care is wireless therefore this may result unsafe for the organization as there may be various security threats. Threats may be with respect to system and information.[ix]The internal threat may be eves dropping or modification of data or privacy issues.

- **Malware for Business Houses -** Business houses and individuals are facing sophisticated malware attacks around the world[x]. This is true about not only big business companies but even small and medium business houses. Cyber criminals are also targeting individuals for sensitive personal and financial information. Ransom attacks are increasing and they are targeting stakeholders ranging from big hospitals, banks and individual computer users.

- **Cyber Threats faced by IT Companies**: Backdoor Attacks, Denial of Service Attack, Direct-Access attacks, Eavesdropping, Spoofing, Tampering, Privileged escalation, Phishing, Click jacking, Social Engineering, Systemical risk: Financial Systems, Utilities & Industrial Equipment.

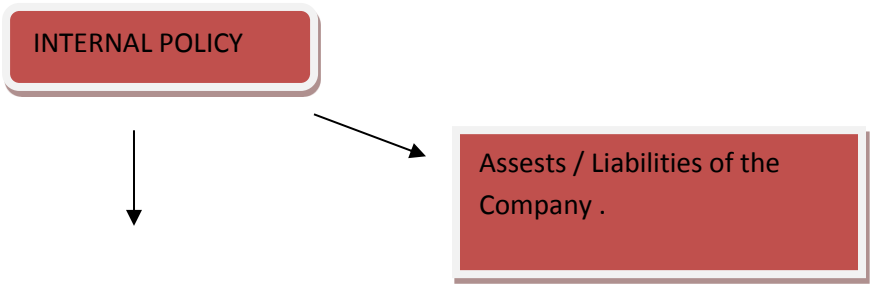
The main motive is to prevent attacks before they are out of control. There is a need to have effective in-house policy to curb such menace.

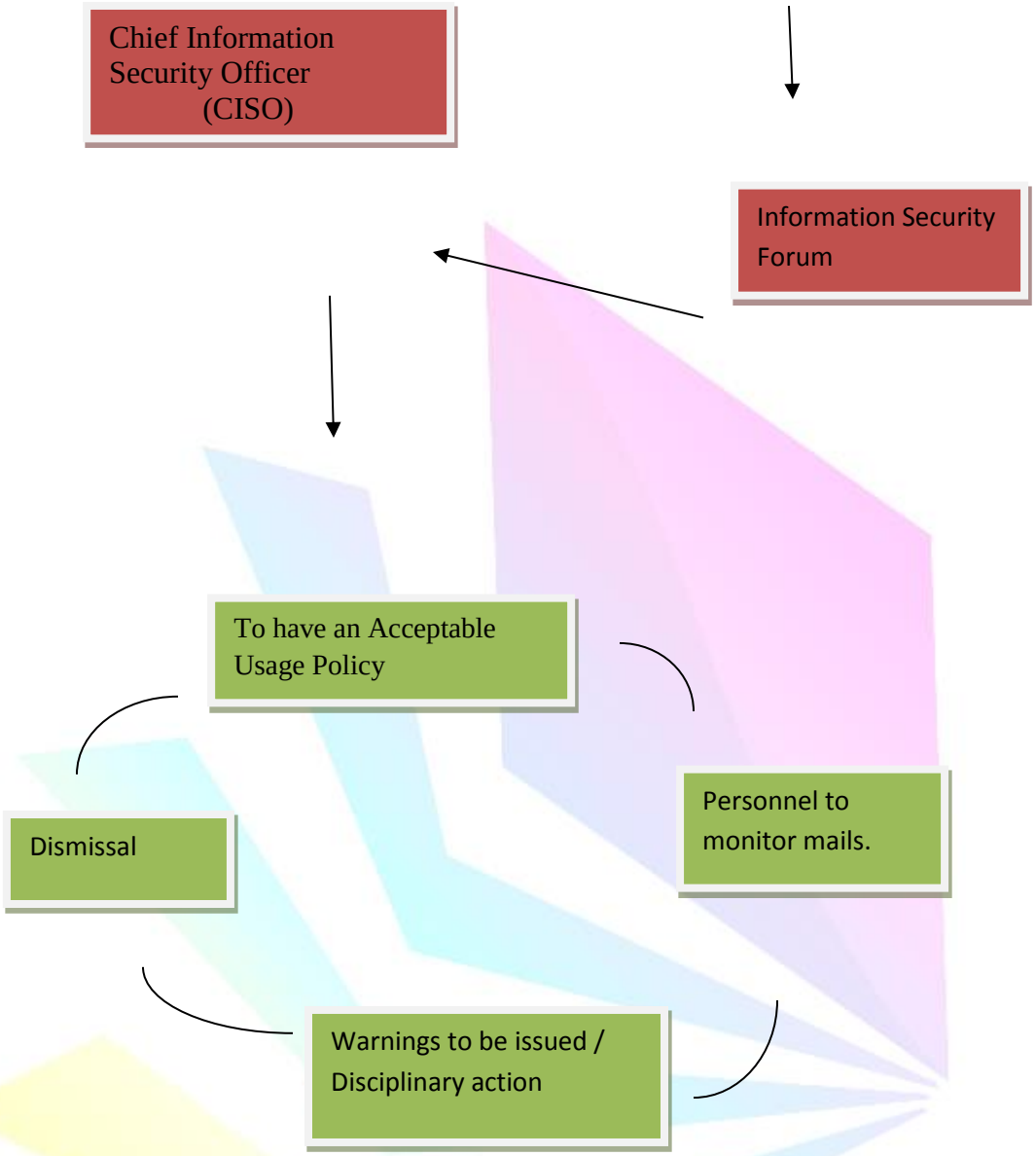
Prevention of Issues on Cyber Security:

1. **Adequate I.T usage policy**: The purpose of the policy is to protect the information assets owned and processed by the Organization from all threats, whether internal or external, deliberate or accidental, to meet all business, regulatory and legislative requirements. This policy is issued with authority of the Information Security Forum (ISF) and owned by Chief Information Security Officer (CISO) of the Organization. Its compliance is mandatory for all users (employees, sub-contractors, suppliers) having access to any of facilities or information systems or information owned or processed by the organization.

   Where a breach of the "Acceptable IT Usage Policy" is established, one or more of the following penalties may be imposed on a user responsible for, or involved in the breach:

- Warning
- Formal written warning
- Restriction , revocation or termination of access to network
- Disciplinary actions, which may include dismissal of the employee or termination of a contract





2. **Data Privacy Issues**: Data Protection Laws apply to the processing of Personal Data. The Data Protection Laws do not apply to "personal" Data. India does not have a dedicated Personal Data Protection Laws. [xi] These are a threat not only for big business houses but also for the small ones, which makes it difficult to survive in the twenty- twenty era. The cybercriminals are using code to lock the data and are holding business houses for ransom for permitting to use their personal data.

Personal Data may only be processed when it is permitted by law and for a legitimate purpose (for example processing of employees' bank details for payroll management purposes, processing of clients' Personal Data for invoicing purposes).

3. **Data Controller & Data Processor**: The Data Controller determines the purposes and means of the processing of Personal Data and decides what data will be collected. Often the Data Controller is the company which originally collected the Personal Data from the individual. The Data Processor processes the Personal data on behalf of the Data Controller. The company that is carrying out the processing asked or instructed to by the Data Controller will usually be the Data Processor.

4. **Data Loss Prevention:** With the changing industry demands and our contractual obligations with clients require that confidentiality of client information safeguarded it is top priority. Equally, also the same is applicable to Organizations' Intellectual Property (examples are client confidential documents, training materials, architecture documents, policy/process documents, functional specifications, source code, customer list, client customer data, personal information (PII) like DOB, Govt. ID, SSN, Credit/ Debit card data). DLP software is designed to detect potential data loss and prevent them by monitoring, detecting and blocking data while in use, in motion and at rest.

   Many Organizations has implemented a DLP application to monitor data loss of company or client confidential data at the network layer (email and web traffic).

Legal Governance of Information

In India, such kind of information is protected under the Trade Secrets and Confidential Information. Yet protection of such information is in the jurisdiction

of the employees. Top priority of every business organization is to protect its information, technology, know-how, customer list and legal data. Though there are no land mark cases protecting trade secrets in India yet there is a need to have laws to protect online data under the Information Technology Act, 2000.

Research Methodology

The author has used the random sampling method to conduct the research. At random, the cyber security in charge, have been interviewed and posed questions related to the subject matter. Based on observations the conclusion has been reached. Further the measures have been laid down which act as a guidelines to business houses to incorporate in their organization.

Observations:

It is observed that most of the organization has an internal chief Security of information, officer appointed by the company. There is an internal policy which guides the employees and is under the jurisdiction of the Chief Security of Information Officer of the company. The compliance of which is mandatory for all the employees, including suppliers, who have access to all kind of company's information. They have an acceptable usage policy, the purpose of which is to protect the information owned by the company. Such a policy is applicable to all users. The users not only include in house but also those delivering information from clients location. Further the policy norms/ document is published on the organization's intranet or the central repository, which is accessible to all employees.

Penalties

The policy further prescribes a set of penalties which includes termination to that extent or any form of disciplinary action. Every user has certain responsibilities as being an employee of the organization.

Responsibilities

There are certain responsibilities which are imposed on the users of the company.

1. To maintain information security this is mandatory for all employees.
2. Compulsory for all the users to maintain and understand security requirements and protect information assets.
3. Employees to maintain secrecy of the I.T facilities of the organization so as to not to disclose it to anyone outside the organization.
4. A team is made to monitor all the systems.
5. Every access must be under authorization.
6. A Helpdesk is created, where all complaints are undertaken with respect to internet security.
7. Companies email ids are provided to all the users.
8. A listing of prohibited sites is made, where access is denied. They are
    i. Sexually Explicit messages
    ii. Love letters
    iii. Racial Slurs.
9. All emails going outside are monitored.
10. Any form of impersonation is regarded as a crime and liable to strict punishment.

Conclusions

There is recourse to the Law or the legislation in India with respect to private and secretive information. There is strict adherence made by the employees of the company to follow the security policies devised by the organization. To conclude, that the Indian legislation need amendments to protect internal, confidential

information. The whole liability rests on the employer and the organization. Tough internal steps are taken by every organization to have internal

[i] Suleman Ibrahim," Socio and Contextual Taxomy of Cybercrime : Socioeconomic Theory of Nigeria cybercriminals." Elsevier, Available on http://www.sciencedirect.com/science/article/pii/S1756061616300787

[ii] http://sponsoredcontent.wsj.com/pwc/broader-perspectives/how-denial-of-service-attacks-wreak-havoc-on-websites/

[iii] http://www.internetlivestats.com/internet-users/

[iv] Information Technology Act, 2000.

[v] Mrs. Rajlakshmi P Wagh," Technological Progress in Branding – A Case Study and Cyber Management", International Journal of Advance Research, IJOAR.Org. Available on http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.678.411&rep=rep1&type=pdf

[vi] Mrs. Rajlakshmi P Wagh, "Comparative Analysis of Trends of Cyber crime Laws in USA and India", International Journal of Advanced Computer Science and Information Technology, Cloud Publication ISSN 2320- 0235. Available on : http://technical.cloud-journals.com/index.php/IJACSIT/article/view/Tech-160/pdf.

[vii] http://www.nasscom.in/initiatives/coe-iot

[viii] *State vs. Mohd. Afzal and Ors*. MANU/DE/1026/2003.

[ix] Moshaddique Al Ameen , Jingwei Liu, Kyungsup Kwak, " Security and Privacy Issues in Wireless Sensors Networks for Healthcare Applications", Journal of Medical Systems, Feberuary 2012 , Volume 36, Issue 1 , pp 93 – 101.

[x] Cyber Security Issues in India. Also Available : http://cybersecurityofindia.blogspot.in/2016/05/malware-are-big-Nuisance-for-businesses.html.

[xi] Perry4Law, " Data Protection Laws In India and Privacy Rights in India". Also Available :http://ptlb.in/clpic/wp-content/uploads/2014/01/Data-Protection-Laws-In-India-And-Privacy-Rights-In-India.pdf.