Information Security At Cyber Space And Integral Component Of Cyber Law With Respect To Domain Security

Sachin Patil
Dr. D. Y. Patil Institute Of Management & Research, Pimpri, University of Pune, Pune, India.
sachpati@gmail.com,

Kalpana Salunkhe
Dr. D. Y. Patil Institute Of Management & Research, Pimpri, University of Pune, Pune, India.
kbsalunkhe2000@yahoo.co.in

Murlidhar Dhanawade
Sinhgad Institute of Business Administration & Computer Application, Lonavala, University of Pune, Pune, India.
harshyash23@yahoo.co.in

ABSTRACT-In recent years, there has been a worldwide wave of using e-government as a mechanism to improve government's efficiency through transparency, openness and increasing interactions across governments, citizens, and the civil society organizations. However, most countries have failed to progress towards achieving its target as envisaged in its information technology (IT) policy documentations. The inability of the national parliament to enact an IT law is primarily considered responsible for such a failure.

KEYWORDS- ICT, Information Security, Cyber Law

I. INTRODUCTION : INFORMATION SECURITY

Governments all over the world have started resorting to the newly found information and communication technology (ICT) to establish a citizen-centric, more transparent and more accountable government mechanism. Available ICT infrastructures together with the government's willingness to implement e-governance has already brought succession e-government initiatives across the industrialized world (Robins & Burn, 2001) [1]. While some developing countries have taken steps in this regard, they often fall short of expectations in improving their governance structure and relevant outcomes. In this regard, a number of barriers exist that need to be understood and tackled by developing countries in pursuing e-government objectives. Including e-government bolstering trust and confidence across the various stakeholders of e-government, viz., the government, citizens, businesses and the members of the wider civil society including non-government organizations (NGOs).

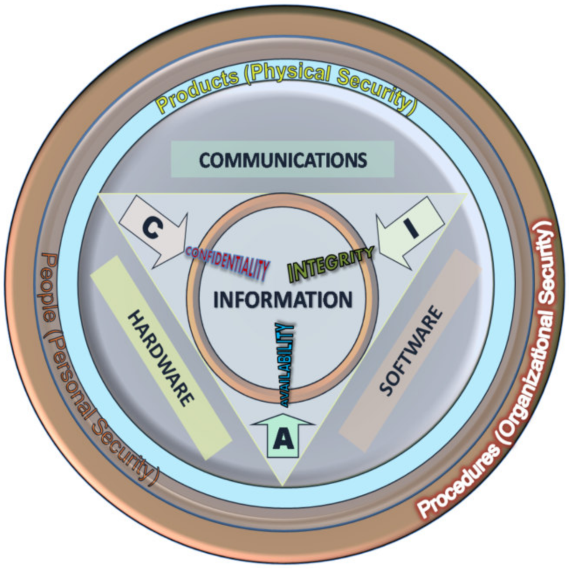
Products (Physical Security)
COMMUNICATIONS
C
I
CONFIDENTIALITY
INTEGRITY
INFORMATION
HARDWARE
AVAILABILITY
SOFTWARE
A
People (Personal Security)
Procedures (Organizational Security)

Figure No. 1Information Security detail

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are often interrelatedand share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them. The field of information security has grown and evolved significantly in recent years. There are many ways of gaining entry into the field as a career. It offers many areas of specialization including: securing network(s) and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning and digital forensic science, etc.

II. INFORMATION SECURITY AND INTEGRAL COMPONENTS OF CYBER LAW

Since the early days Military Commanders felt it necessary to provide some mechanism to protect the confidentiality of written correspondence and to have some means of detecting tampering. World War II marked the advancements in Information Security which was the beginning of the professional field of information security. The early years of the 21st century have brought more and rapid advancements in telecommunications, computing hardware and software, and data encryption. The availability of smaller and more powerful and less expensive computing equipment made electronic data processing within reach of small business and the home user. These computers quickly became interconnected through a network generically called the Internet or World Wide Web. The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are often interrelated and share the common goals of protecting the confidentiality, integrity and availability of information, however, there are some subtle differences between them.These differences lie primarily in the approach to the subject, the methodologies used and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic print, or other forms. Should confidential information about a business customers or finances or new product line fall into the hands of a computer, such a breach of security could lead to loss of business, law suits or even bankruptcy of the business. Protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement [2] [3].

Basic Principles

a. Confidentiality

This is a term used to prevent the disclosure of information to unauthorized individuals or systems.

Example : A Credit Card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encryptting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts etc.) and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality occurs.There are many forms of Breach of Confidentiality : Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality.

- Integrity
- Availability
- Authenticity
- Non-repudiation

b. Risk Management

“ Risk Management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take a reducing risk to an acceptable level, based on the value of the information resource to the organization.”

There two things in this definition :

1.Ongoing interactive process. The business environment is rapidly and repeatedly changing and new threats and vulnerability emerge.

2. Countermeasure (computers) controls used to manage risks must strike a balance between productivity , cost effectiveness of the countermeasure, and the value of the information asset being protected.

Risk is a vulnerability that causes harm to an informational asset. A threat is anything (man made or act of nature) that has the potential to cause harm. A risk management is carried out by a team of people who have knowledge of specific areas of the business. Membership of the team may vary over time as different parts of the business are assessed. The assessment may use a subjective qualitative analysis based on informed opinion, or where reliable dollar figures and historical information is available, the analysis may use quantitative analysis [4].

- Administrative
- Logical
- Physical

c. Security Classification For Information

An important aspect of information security and risk management is recognizing the value of information and defining appropriate procedures and protection requirements for the information. Not all information is equal and so not all information requires the same degree of protection. This requires information to be assigned a security classification.

The first step in information classification is to identify a member of senior management as the owner of the particular information to be classified. Next develop a classification policy.

- Access control
- Identification
- Authentication

There are three different types of information that can be used for authentication:

Something you know- e.g. PIN , a Password, or your mother's maiden name. Something you have- e.g. A driver's license, a magnetic swipe card.

Something you are - e.g. Biometrics include palm prints, finger prints, voice print And retina (eye) scans.

d. Cryptography

Information security uses cryptography to transform usable information into a form that renders it unusable by anyone other than an authorized user; this process is called ENCRYPTION. Information that has been encrypted (rendered unusable) can be transformed back into its original usable form; an authorized user, who possess the cryptographic key, through the process of decryption. Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit (either electronically or physically) and while information is in storage[5][6]. Cryptography provides information security with other useful applications as well including improved authentication methods, message digests, digital signatures, non-repudiation , and encrypted network communications. Older less secure applications such as Telnet and ftp are slowly being replaced with more secure applications such as ssh and that use encrypted network communications. Wireless communications can be encrypted using protocols such as WPA/WPA2 or the older (and less secure) WEP, Wired communications (such as ITU-T.G. h n) are secured using AES for encryption and X.1035 for authentication and key exchange. Software applications such as Gnu PG or PGP can be used to encrypt data files and Email [7].

e. Business Continuity Plan

Business Continuity is the mechanism by which an organization continues to operate its critical business units, during planned or unplanned disruptions that affect normal business operations, by involving planning and managed procedures.Unlike what most people think business continuity is not necessarily an IT system or process, simply because it is about the business. Today disasters or disruptions to business are a reality. Whether the disaster is natural or man-made (the TIME Magazine has a website on the top 10), it affects normal life and so business. So why is planning so important ? Let's face reality that "all business recover" , whether they planned for recovery or not, simply because business is about earning money for survival.For business to create effective plans they need to focus on the following key questions. Most of these are common knowledge, and anyone can do a Business Continuity Plan [8] [9].

f. Disaster Recovery Planning

While a Business Continuity Plan (BCP) takes a board approach to dealing with organizational-wide effects of a disaster, a disaster recovery plan (DRP) , which is a subject of the business continuity plan, is instead focused on taking the necessary steps to resume normal business operations as quickly as possible. A disaster recovery plan is executed immediately after the disaster occurs and details what steps are to be taken in order to recover critical information technology infrastructure.

III. CONCLUSION

E-government in developing countries is going through a process of transition. However, despite such intention and apparent enthusiasm, the creation of a citizen-centric, transparent and efficient digital society based on e-government & information security concepts. Process and has failed to demonstrate its ability to progress towards the higher phases of e-government, i.e., 'transaction' followed by 'transformation'. Given the increasing complexity and costs involved in moving towards the higher levels, a strong politico-administrative framework with the ability to frame and enforce the law is considered as an important precondition to establish an ICT-driven government. In addition to providing legal recognition to important e-government functions such as e-communication and e-transactions, an effective legal framework is required to create an environment conducive to promoting and executing e-government. It also offers safeguard to intellectual property and copyright of e-publications and helps identify, define and prevent the various e-criminal activities. Therefore, an appropriate legislations of an IT Act together with streamlining and linking other relevant legal codes are important in order to restrain and remedy crimes such as threats against property and individuals, piracy, hacking and fraudulent activities and illicit transfer and posting of data on the web (eg., viruses and pornographic materials),. In addition, the specific legal authority needs to be exercised in order to protect intellectual property including Copyrights. With respect to data security and interoperability, an appropriate legislation is required to be enacted to establish encryption standards and to accommodate international agreements on interoperability (MOSICT, 2002). It is, therefore, the time for developing countries to come forward and immediately enact the ICT Act to facilitate government and integrate it to the global e-revolution.

REFERENCES

[1] PublicManagement and Citizens' Rights. Edward Elgar Publishing Limited, Cheltenham. Cabinet okays draft of ICT act 2005. The Daily Star. 2005, February 15. Retrieved June 10, 2006,from http://www.thedailystar.net/2005/02/15/d5021506118

[2] Burkert, H. 2004. The mechanics of public sector information. In G. Aichholzer & H. Burkert (Eds.), Public Sector Information in the Digital Age: Between Markets

[3] Cyber Law In India, Dr. Faruq Ahmed

[4] Computer, Internet And E-commerce, Mr. Nandan Kamat.

[5] Cyber squatting: Pits & Stops, S.AHMED

[6] Indian Law, Cyber Law Girish Ahuja

[7] Cyber Law / Evidence Act, O. P. Agarwal.

[8] Cyber Law & Cyber Security

[9] www.securitygovernance.net Cyber Case Study