International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 5 | ISSN : 2456-3307

A Strategical Transition from Information Security to Cyber Security

Rashmi B H
Assistant Professor, Department of Computer Science & Engineering, Global Academy of Technology
Bangalore, Karnataka, India

ABSTRACT

Cybersecurity is gaining more popularity in the field of Computer science and network security due to change in the technologies and development. Basically Cybersecurity deals with the protection of computer systems from threat, various malwares, theft or damage to hardware or software data. Cybersecurity is also termed as Computer security or IT security. Cybersecurity is gaining wider acceptance because of increasing reliability on Computer systems, Internet, Wi-Fi and most importantly due to the substantial growth of Smart devices. Moreover there is a great overlap among Information security and Cybersecurity. The paper more urges on Cybersecurity whose security boundaries goes beyond Information security. Cybersecurity not only protects resources but also focuses on securing the personal assets of the humans. Information security describes the role played by humans in protecting the computer system from unauthorized access or use, whereas Cybersecurity particularly targets on humans, because humans are referred to as potential targets on Cyber-attack, i.e.; knowingly or unknowingly people would be involved in Cyber-attack. Therefore this additional feature of Cybersecurity has a profound implications on society, since the protection of certain vulnerabilities and humans, especially children is a major social responsibility.

Keywords : Cybersecurity, Information security, Cyber-attack, Computer security, Threat, Vulnerability.

I. INTRODUCTION

Cybersecurity is gaining wide acceptance and popularity among changing technologies in order to impose security in managing human interactions with social media. Cybersecurity consists of tools, policies and certain security principles to be imposed in order to enforce and maintain security. Cybersecurity deals with managing human assets, policies and secures the infrastructure with the help of certain safeguard principles and rules. Cybersecurity consists of modern technologies to safeguard cyber environment and organization assets. The main aim of Cybersecurity deals with the maintenance of organization and user's asset against certain harmful threats and malicious contents. General security policy consists of CIA triad

(Confidentiality, Integrity and Availability) which is as follows:

- **Availability**- It refers to the user ability to access various information and resources in a specified location in the standard format.
- **Integrity**- In computer security, Integrity refers to the methods of ensuring that the data is accurate and real and is being monitored against unauthorized access.
- **Confidentiality**- It is a mechanism which allows only authorized users to access protected data and resources.

The above definitions discussed regarding CIA triad are very much similar to those definitions of Information Security. This paper will explain about Information security and tells how Cybersecurity concepts are much wider than Information security.

This paper will particularly concentrate on various aspects of Cybersecurity, as it aims to protect the Computer system by adding an additional feature of including both humans and society, wherein both are directly affected by various cyber-attacks.

II. BACKGROUND

China is very much associated with various types of cyber-attacks and cybercrimes. So the paper mainly focuses on various technologies, topologies and various classification methodologies of Cybersecurity to safeguard the country from various attacks. It involves many characteristics of cybersecurity organizations, gains information regarding china human growth statistics and culture to analyze various aspects and enforce various Cybersecurity mechanisms to provide security [1].

Many approaches to Information security are not working up to the mark and not producing more security to safeguard various organizations. Because of the various multi-dimensional security features, Information security principles are lagging behind. To overcome these various Cybersecurity tools are being developed and used to provide national security to safeguard computer system or organization [2].

Information security developed a simple Intrusion detection system and anomaly detection technique to safeguard the organization's computer systems. The major drawback raised is, these systems were only applicable to simple network and were not able to perform deep packet inspection and couldn't avoid malicious threat or contents entering into the network. With the advent of new tools and techniques related to Cybersecurity, accurate detection of malicious contents could be done and also with the help of these tools deep packet inspection could be carried out [3].

Computer systems are experiencing more number of security attacks and threats. Managing network security with the increase of new types of attacks is an open challenge and is becoming tedious task. So to overcome these disadvantages, an improved version of anomaly based intrusion detection system involving Cybersecurity techniques should be developed [4].

III. INFORMATION SECURITY

The primary focus of Information security is to prevent illegitimate access, modification of data and avoiding certain threats entering into the network. The main aim of Information security is to minimize the damages caused in business community. Information security basically enforces limited security features. The main functionality of information security is to follow the principles of CIA Triad as shown in the Fig1.

Figure 1: CIA Triad

Information security functionalities include securing databases, security testing, maintaining software's, application testing and data maintenance and avoiding certain threats entering into the network as shown in the Figure 2.

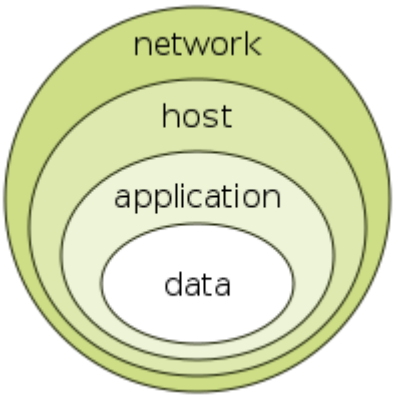

Figure 2 : Functionalities of Information Security

Information security threats comes in many different forms. Common examples of Information security threats are certain software attacks, theft of intellectual data, viruses and some kinds of Trojan attacks.

Various Definitions of Information Security

Information security can be defined in many ways as follows:

- Information security is defined as the "Process of preserving data integrity, confidentiality, authenticity and availability of Resources".
- Information security involves in the "Process of protecting the Information from illegitimate access, modification of data and disruptive use of data".
- Information security "Ensures that only authenticated and authorized users should access the data and the accessed data should be available when required".
- Information security follows the principle of Risk management, where it minimizes the risk and maintains the cost related to business community.
- Information Security is a multidisciplinary area of study which implements new tools, techniques and mechanisms to enforce security in any organization.

The Basic principles of Information security involves

- Confidentiality
- Integrity
- Availability
- Non-repudiation.

Advantages and Disadvantages of Information Security

Advantages:

- Easy to utilize. Information security helps in preserving less sensitive data.
- Information security preserves Private information.
- Information security preserves the data when it is used or wen it is being stored.

Disadvantages:

- As the technology is changing eventually, user must always use the upgraded security policies of Information security in order to perform maintenance of resources.
- If a particular user misses any area of network to be protected, then the whole system will be affected.
- Sometimes the process becomes highly complicated.
- Slows down Productivity.

IV. CYBERSECURITY

Cybersecurity deals with the process of preserving the computer system from certain viruses and disruption of services. The major difference between Information security and Cybersecurity is that Information security has its primary focus on protecting the company data from illegitimate access or unauthorized access whereas Cybersecurity deals with the protection of company data from unauthorized electronic access. So in both concern value of Data is of great importance. Cybersecurity protects the Cyber environment of a user as well as the Organization. The difference among Cybersecurity and Information security is as shown in the Figure 3.

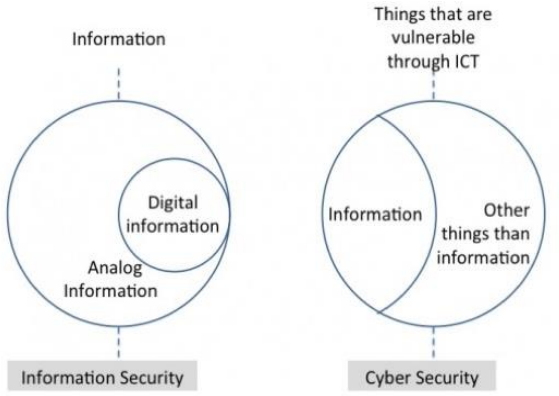

Figure 3 : Difference among Cybersecurity & Information security

More precisely Cybersecurity can be defined as the process of protecting the Cyberspace environment from cyber-attacks. Information security as the name suggest, is defined as the protection of Information and Information systems from illegitimate access, restricted use and disruption. Information security protects any sort of Physical information or computerized information, whereas Cybersecurity deals with the protection of Cyberspace environment against any type of crime related or not related to CIA triad.So in a common term Cybersecurity deals with the protection of Both information and also cyberspace environment(involving Humans) from various Cyber-attacks.

From the above Venn diagram, Cybersecurity explains that it deals with the protection of certain things which are vulnerable through ICT (Information and Communication Technologies).It protects both physical and digital information or data and non-information such as Electronic devices, whereas Information security only deals with the protection of Analog and Digital information only.
The following emerging scenarios explain the importance of Cybersecurity.

- **Traditional growth of Internet-of-Things:**

IoT is gaining wide importance nowadays, as a result vanishing the physical and virtual world. This advancement has results in many online risks further making a huge contribution to various types of Cyber-attacks. Henceforth Cybersecurity mechanisms are taken up to prevent certain real time social networking attacks in cyberspace environment.

- **Traditional Business entities under pressure:**

Intellectual property enables traditional business entities under pressure by evolving new technologies with new competitors. As a result established market leaders fall and new advancements and new vendors rise up in these environment. Therefore cybersecurity mechanisms must be enforced to protect various types of data stored.

- **Intended Growth of public-private partnerships:**

Organizations tend to know more about their customers regarding data sharing both publicly and privately. This procedure can be advantageous to national security but at the same time results in an error because more organizations are Foreign based. So due to this national security becomes critically complicated.

- **Citizens demand Transparency:**

Citizens are demanding greater control and transparency over their online data. Nowadays people who are technically weak don't preserve integrity and confidentiality of data and would leak the information for cost benefits. So citizens are demanding a transparent network and a cybersecurity mechanisms to safeguard their data.

- **Cyber-resilient Organizations:**

Cyber-resilient organizations are very important to prevent and alert business organizations from inside threats and certain Cyber-attacks. In order to get rid of these attacks Cybersecurity is gaining much importance to ensure security policies to prevent business organizations from Cyber-attacks.

From the above scenarios it is necessary to frame Cybersecurity framework to enforce security policies

and to impose some Cybersecurity laws in order to prevent humans and also information from Cyber-attacks.

V. TRANSITION FROM INFORMATION SECURITY TO CYBERSECURITY

Security as the name suggests, is the protection of assets from various threats and certain vulnerabilities. Information security only protects the information or data (physical or digital).Therefore the information security does not go beyond the technology of protecting the information which is being communicated or stored using ICT.

In the Cybersecurity, the assets need to be protected can range from information/data (physical or digital), electronic devices and also humans in social environment. From the above scenarios, it is concluded that Cybersecurity protection goes beyond that of information security boundaries. Cybersecurity protects the assets (both tangible and intangible) related to physical and personal aspects related to human society.

Cybersecurity is not just about the protection of Information or data but also information or computer system related to a person or a business organization. Cybersecurity also protects the humans accessing the resources in cyber space environment from various Cyber-attacks. The pictorial representation of Cybersecurity and Information security is as shown in the Figure 4

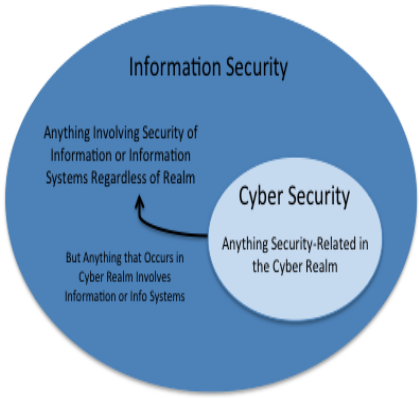

Figure 4: Cybersecurity & Information security

Therefore it is clear from the above discussions that Information security is meant for the protection of assets related to information or data within the defined boundaries, whereas Cybersecurity deals with the protection of assets related to information and also to secure the functionalities in cyber space environment.

VI. CONCLUSION

The paper explored the definitions of Information security and Cybersecurity. The paper also explained the differences among Cybersecurity and Information security. Information security is the protection of information or data from certain threats and vulnerabilities. Cybersecurity is the protection of not only the data or information but also the functionalities and human society functioning in Cyberspace environment.

VII. REFERENCES

1. Nir Kshetri,"Cybercrime and Cyber-security Issues Associated with China: Some Economic and Institutional Considerations", Electronic Commerce Research 13 (1): 41-69.
2. Myriam Dunn Cavelty," Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities", Springer Science +Business Media Dordrecht 2014.
3. Noam Ben-Asher, Cleotilde Gonzalez," Effects of cyber security knowledge on attack detection", 0747-5632/_ 2015 Elsevier Ltd. All rights reserved.
4. PGarci-a-Teodoroa,,J.Di-az-Verdejoa, G. Macia--Ferna-ndeza,E.Va-zquezb, Anomaly-based network intrusion detection: Techniques, systems and challenges", 2008 Elsevier Ltd.