Cyber Security: Need of the Hour

Dr. Sushma H.B.

Sushmahaigar@gmail.com

09980095126

ABSTRACT

Due to the advent of information and communication technology (ICT) in 21st century, there is a tremendous increase in the usage and dependency on cybernate in all sphere of human life. On the account of inevitable material and infrastructural growth, there is a need inherent also to get secure the said infrastructure using advanced technologies by keeping a proper vigilance in order to prevent the top secrets being penetrated and hacked. In this race vast burden is on cyber experts to protect such confidential infrastructures, which are prone to cyber attacks and threats increasingly. This paper tries to unfold the meaning of cyber security with main objectives as to know principles of cyber security, to know how one will be at risk, to know the needs of cyber security, to know the advantages of cyber security and to create awareness. To have a safe nation, safe cyber security is needed.

Key Words: Cyber security, Information and communication technology.

INTRODUCTION:

Information and communication technology (ICT) is enabling transformation, the way government, industries, health and business sectors, general public organization and educational institutions, communicate, exchange knowledge, skills, process , use and store information and conduct their everyday lives. Thus analysis shows increased use of ICT's and dependency for greater productivity and better livelihood is increasing day by day, thus making very one too difficult to image our nation which is critically dependent on ICT in an analogous manner to that of our basic physiological needs , without which we cannot survive. The harsh reality is, we are heading towards a third world war and every country has a need to put its citizens under surveillance simultaneously no country in these modern days could afford to be delinked with outside world and in this pursuit the issue of privacy versus security has become a hot subject around the world.

NEED OF THE STUDY

Usage of Internet has become an integral part of human life in the modern world. From communicating via email and instant message to traveling, banking and shopping, nearly every aspect of our life revolves around the cyber world. Because the Internet is so widely used, protecting vital information in the cyber world is not only our responsibility, but a necessity to preserve our national security. Hence this study has been taken up.

STATEMENT OF THE PROBLEM

"Cyber Security: Need of the Hour"

OPERATIONAL DEFINITIONS OF KEY TERMS

Cyber Security:

Is the activity of protecting information system (networks, computers, data bases, data centers and application) with appropriate procedural and technological security measures. In that sense, the notion of cyber security is quite generic and encompasses all protection activities. Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.

Information and Communication Technology:

ICT which means computers, mobile phones, digital cameras, satellite navigations systems, electronic instruments and data recorders, news paper, radio, television, computer networks, satellite systems almost anything which handles and communicates information electronically. ICTs, not only refer to the latest computer and internet based technologies, but also to simple audio visual aids such as the transparency and slides, tape and cassette recorders, videocassettes, television and film. These older are grouped under "analogue media" while the newer computer and internet based technologies are called the "digital media". ICT includes both the hardware (the equipment) and the software (the computer programs in the equipment).

Is an umbrella term that includes any communication device or application, encompassing radio, television, cellular phones, tab, computers, laptop, network hardware, software, satellite systems and so on, as well as the various services and applications.

REVIEW OF LITERATURE

Alexander Klimburg (2012) ICT security is more directly associated with the technical origins of computer security, and is directly related to 'information security principles' including the confidentiality, integrity and availability of information resident on a particular computer system. (DSTO: Science and Technology for Safeguarding Australia) reported, Cyber threats are potential cyber events emanating from unintentional actions or as a result of attacks developed by malicious parties that exploit vulnerabilities and cause harm to a system or organisation. Understanding both existing and emerging threats is vital for the future development and correct operation of information systems

OBJECTIVES OF THE STUDY

01. To know principles of cyber security
02. To know how one will be at risk
03. To know the measures to protect from risk
04. To know about cyber security threat.
05. To know the importance and needs of cyber security
06. To create awareness regarding cyber security
07. To know the advantages of cyber security

01. To know principles of cyber security

There are three core principles of cyber security:

a. **Confidentiality:** Information which is sensitive or confidential must remain so and be shared only with appropriate users. For example, your confidential medical records should be released only to those people or organizations (i.e. doctor, hospital, insurance, government agency, you) authorized to see it (confidentiality).

b. **Integrity:** Information must retain its integrity and not be altered from its original state. The records should be well protected so that no one can change the information without authorization (integrity)

c. **Availability:** Information and systems must be available to those who need it. The records should be available and accessible to authorized users (availability).

02. To know how one will be at risk

Unauthorized users that invade a system are commonly known as hackers, and hackers have a wide variety of tools to harm a computer system. Hackers usually gain access to systems by planting malicious logic (like a virus) somewhere on the net and waiting for users to encounter or open the virus. Common ways a computer can become infected are:

- Opening an email attachment that contains malicious logic
- Visiting a malicious website
- Clicking on a dangerous link
- Inadvertently downloading a harmful program

Infected computer systems may be affected and damaged in a variety of ways, sometimes without a user even noticing. Some hackers are “playing a prank,” while others may be attempting to steal personal information such as credit card numbers, Social Security numbers, or other personal information. Even worse, hackers can take control of an infected computer and use it to launch an attack on a larger system. Even if your computer has no stored sensitive data, it can still be used to infect other computers without your knowledge! This practice is so prevalent that access to vulnerable or infected computers is bought and sold among hackers.

03. To know the measures to protect from risk

To protect from risk one should recognise the risk and become familiar with some terminology associated with them, like hacker, attacker or intruder – These terms are used to those persons who seek to exploit weaknesses in software and computer systems for their own benefits. This results from mere mischief (creating virus with no negative impact) to malicious activity (stealing or altering information). Another measure to protect is to use the cyber security standards, which enable organizations to practice safe security techniques to minimize the number of successful cyber security attacks. These guides provide general outlines as well as specific techniques for implementing cyber security. For certain standards, cyber security certification by an accredited body can be obtained. Cyber security standards have been created recently because sensitive information is now frequently stored on computers that are attached to the Internet. Also many tasks that were once done by hand are carried out by computer; therefore there is a need for Information Assurance (IA) and security.

04. To know about cyber security threat

Three types of threats act upon cyber security

- **Software based** - Viruses, worms, spyware, root kits, exploit scripts, protocol exploits.
- **Hardware based** - Hardware Trojans, counterfeit components
- **People** – Insider and outsider threats either from malicious or inadvertent actions or inaction.

These threats can affect data at any stage – During storage, when it is being processed, when it is in transmission across the network or when it is accessed via personal computer, mobile devices, or other end point devices. They attack the confidentiality, integrity and availability of information, information systems and hardware through

- Unauthorised revealing of information (loss of confidentiality)
- Unauthorised modification or destruction of information (loss of integrity)
- Disturbance in accessing, to use of information or an information system loss of availability.

05. To know the importance and needs of cyber security

Governments, military, corporations, financial institutions, hospitals and other businesses collect, process and store a great deal of confidential information on computers and transmit that data across networks to other computers. With the growing volume and sophistication of cyber attacks, ongoing attentions is required to protect sensitive business and personal information, as well as safeguard national security.

06. To create awareness regarding cyber security

Most hackers use malicious logic to exploit vulnerabilities in software and gain unauthorized access to computer systems. For this reason,

a. It is vitally important to install and update anti-virus, anti-spyware and firewall software. Because new vulnerabilities in computer systems are found every day, computer companies "patch" these vulnerabilities by issuing a series of system updates.

b. To ensure your computer is safe from known vulnerabilities, make sure to install all updates on a regular basis.

c. A strong password that has at least nine characters, contains a capital letter, uses a special character (such as #, %,*) and includes a number.

d. Consistently track your credit information so that if your computer is infected, you can minimize damage.

e. Back up important information on your computer.

f. Scan your computer for viruses, spyware and other vulnerabilities on a routine basis.

g. Be cautious about all communications; think before you click. Use common sense when communicating with users you DO and DO NOT know.

h. Only visit websites you trust, and open emails only from known contacts.

07. To know the advantages of cyber security

The increasing volume and sophistication of cyber security threats–including targeting phishing scams, data theft, and other online vulnerabilities–demand that we remain vigilant about securing our systems and information. The average unprotected computer (i.e. does not have proper security controls in place) connected to the Internet can be compromised in moments. Thousands of infected web pages are being discovered every day. Hundreds of millions of records have been involved in data breaches. New attack methods are launched continuously. These are just a few examples of the threats facing us, and they highlight the importance of information security as a necessary approach to protecting data and systems.

CONCLUSION

Many aspects of our lives rely on the Internet and computers, including communications (e-mail, cell phones, texting), transportation (traffic control signals, car engine systems, airplane navigation), government (birth/death records, social security, licensing, tax records), finance (bank accounts, loans, electronic paychecks), medicine (equipment, medical records), and education (virtual classrooms, online report cards, research). Consider how much of your personal information is stored either on your own computer or on someone else's system. How is that data and the systems on which that data resides (or is transmitted) kept secure? Cyber security involves protecting the information and systems we rely on every day—whether at home, work or school. Securing cyberspace will be harder. The architecture of the internet is designed to promote connectivity, not security. Cyber experts warn that nations that are unprepared to face the threat of a cyber is 9/11. The more technologically advanced and wired a nation is the more vulnerable it is to a cyber attack. Ensuring security of data, information and communication is considered harder than hacking into a system.

Defence against cyber attack is becoming increasingly difficult. This was highlighted at the recent RSA conference 2016 in the U.S. The need of the hour is to accelerate the pace at which cyber security are produced, to meet the growing threat. Thus the issue of privacy versus security of a nation is a "hot" subject around the world. (The Hindu).

REFERENCE

Alexander, k. (2012). National Cyber Security Frame Work Manual. NATO CCD COE publication, (Pp 09**)**.

Introduction to Cyber Security. Uganda National Computer Emergency Response Team. (Pp 1-3).

"Why is Cyber Security Important to me"? Air Force Association.

Future Cyber Security Landscape. A Perspective on the Future. Australian Government Department of Defence. (Pp 04).

News Paper "The Hindu". Saturday, March 19, 2016 (Pp 10)

WEB SITE

www.cybersecurity.alabama.gov