Chapter 1
Role of Cyber Security in Today's Scenario

Manju Khari
NITP, India

Gulshan Shrivastava
NITP, India

Sana Gupta
AIACTR, India

Rashmi Gupta
AIACTR, India

ABSTRACT

Cyber Security is generally used as substitute with the terms Information Security and Computer Security. This work involves an introduction to the Cyber Security and history of Cyber Security is also discussed. This also includes Cyber Security that goes beyond the limits of the traditional information security to involve not only the security of information tools but also the other assets, involving the person's own confidential information. In computer security or information security, relation to the human is basically to relate their duty(s) in the security process. In Cyber security, the factor has an added dimension, referring humans as the targets for the cyber-attacks or even becoming the part of the cyber-attack unknowingly. This also involves the details about the cybercriminals and cyber risks going ahead with the classification of the Cybercrimes which is against individual, property, organisation and society. Impacts of security breaches are also discussed. Countermeasures for computer security are discussed along with the Cyber security standards, services, products, consultancy services, governance and strategies. Risk management with the security architecture has also been discussed. Other section involves the regulation and certification controls; recovery and continuity plans and Cyber security skills.

DOI: 10.4018/978-1-5225-5634-3.ch001

INTRODUCTION

Cyber security known by "information technology security", emphasise on securing networks, data, programs and computers from unauthorized or unintended variation, loss, change or access. Government agencies, corporations, hospitals, financial institution, military and other groups store, gather and practise a big deal of intimate information on the computers and send that data over the network to the other computers. With the growing volume and criticality of cyber-attacks, the emphasis is needed to secure confidential information and trade, also securing the security of nation. Security in Computer also known as "cyber security" either "IT security" which means preservation of information entities from damage or theft of the software, the hardware and to the information cured on them, also from the misdirection or disruption of the duties they offer.

It involves the regulation of the physical approach to the hardware, also preserving from attack that can come from accessing network, code injection & data, and because of illegal activities by vendors, whether intentional, accidental, or due to them by guessing the secure methods. The domain is of developing relevance because of the growing dependency on the internet and computer systems in most of the wireless networks, societies like Wi-Fi, Bluetooth and the growth of intelligent devices, involving televisions, small devices and smart phones as an important section of the IoT. While increased technological developments have given many areas for organisations of all sizes, potential sources of efficiency and better opportunity. Cyber security – explained as the "protection of systems, networks and data in cyberspace – is a critical issue for all businesses". Cyber security will become vital as more number of devices, become connected to the computer internet, 'the internet of things'.

HISTORY OF CYBER SECURITY

Along the several malicious viruses and distinct types of malware in today's scenario, it looks awkward to think that "just a few decades ago, at the birth of networks and the world-wide web, security wasn't always a top concern". Even, in the early steps of ARPANET, "a packet-switched network funded by the Pentagon", many attacks were made by the high school students. Similarly, as it can look to today's scenarios related to TalkTalk, which was earlier when cyber security did not exist, and in a long line of attacks it was the first that forced the computer researchers around the world to implement and act security methods.

"Cyber criminals and network criminals", it looks since we have networks. 'Phreaking', or the process of hacking phone lines to create free calls, was a famous technique used in the 70s and the starting days of the networks. One of the most famous phreakers, John Draper, who used to try and was then punished and arrested due to the repeated attacks. In 1989, "Robert Morris unleashed the first computer worm on the internet, which managed to take down much of what was online at the time". But in the late 80s, the internet was not as vital part of our day-to-day living as it is now, and so the consequences were not as efficient as they would be today. The 'worm' virus became the first crime to be convicted under "the 1986 Computer Fraud and Abuse Act." The worm case incurred publicity after several early viruses had been exposed in the starting 1980's, such as the 'Brain' virus of 1986.