Chapter 72
Proposals to Win the Battle Against Cyber Crime

Alaa Hussein Al-Hamami
Amman Arab University, Jordan

ABSTRACT

Through commercial networks and across the Internet, there are data files, millions of images and videos, and trillions of messages flow each day to drive the world economy. This vast electronic infrastructure is what our nation depends on. To commit crime by using a computer and communication to forge a person's identity, illegal imports or malicious programs, the computer here is used as an object or subject for the cybercrime. Most of the online activities are vulnerable to intrusion and can compromise personal safety just as effectively as common everyday crimes. This chapter concentrates on explaining and discussing the terms of cyber security, cybercrimes, and cyber-attacks. A history for each term has been given and the problems of cyber security have been discussed. Finally, a proposed solution has been suggested and future trends have been forecasted, and at the end of the chapter a conclusion will be given.

INTRODUCTION

A new theories and terms appear to change the concepts of the economics and the role of the organizations in society. Theories such as the "Blue Lake" and terms such as: Network Economics, Virtual Organizations, E-Government, E-Business, and Internet of Things are dependent, in general, on the Internet and Information Technology. New technology always brings new threats and here, security is the main concern for these technologies.

The advances of computers and communications have changed our life and habits. Everything now relies on those developed technologies (computer and Internet), communication (email, mobile phones), transportation (airplane navigation, car engine systems), shopping (e-commerce, credit cards, and online stores), medicine (medical records, equipment), entertainment (mp3s, digital cable) and the list goes on. We can see that our daily lives rely on computers. Also, much of our personal information is stored and processed on our own computers or on someone else's system. The objective of cyber security is to protect and defend that information by detecting, preventing, and responding to cyber-attacks (Ramkumar, 2014).

DOI: 10.4018/978-1-5225-5634-3.ch072

The Internet has 90% junk and 10% good security. When intruders find systems that are easy to break into, they simply hack into the system. Terrorists and criminals use information technology to plan and execute their cyber-criminal activities. The wide spread usage of computers and communications has facilitated the growth of crime and terrorism. Because of the increase in international interaction and the advanced communication, technology people need not be in one country to conduct such crime. Hackers can find security gaps in the system and can function from anywhere instead of their country of residence (Crime Desk, 2009).

The industries have invested considerable effort in managing the risks of terrorism and other deliberate criminal acts against facilities through their computer systems. Random attacks of worms, Trojans, viruses, etc. have occurred and they have adversely impacted computer systems including those operating manufacturing facilities, while few deliberately focused attacks on manufacturing systems have been reported,

THE HISTORY OF CYBERCRIME

Capacity of human mind is unfathomable. It is impossible to eliminate crime from the globe and there is no legislation has succeeded in doing that. People aware of their rights and duties and they know that the application of the laws is more stringent to check crime. Finally, it is not possible to eliminate cybercrimes from the cyber space.

Computers are a tool that criminals use much like a lock picking tool or a counterfeiting machine. Criminals have learned that computers provide an anonymity that has previously been unattainable in society. Criminals are criminals everywhere and at any time and their aims are to gain benefits (financial, social, etc) and at the end harming the society.

An advance in computers and communications that is so radical it not only changes the way that societies interact, it also has fundamental effects on the behavior of the human and criminal element within that society: introducing completely new and previously unheard of actions into our everyday life. Cyber Crime is one of the biggest radical changes in the society and criminal behaviors (Power, 2001).

The computer networks allow cyber criminals to conduct illegal activity from a remote computer far away from the crime position here it taking place by controlling another computer and make it to attack another computer. A criminal can access a computer network a continent away and steal credit card and banking information without having to be physically present at the scene. Criminals are using computers to conduct several crime acts such as: information theft, intellectual property theft, fraud, etc. using a computer and the communications as a subject or an object for illegal activity (Saini et al, 2012).

Cybercrime

Cybercrime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime. Cybercrime is the most complicated problem in the cyber world.

Essentially, there are two separate and distinct components in cybercrime. One component is the exploiting weakness in the computer operating system or network (this method used by Hackers). The second component is the exploiting social fabric of a computer network (this method is called Social