Computer Crimes and Abuse

Saad Abdulghani Shwailah

Abstract—**This topic is to cover the computer crimes and also computer abuse in general. It defines the computer crimes and introduces the set of global and local laws of computer crimes. It also shows some statistics and facts about those crimes and finally it talks partially about hacking which is one of the computer crimes.**

Index Terms— **Computer crimes, cyber crime, hacking, laws of computer crimes.**

I. INTRODUCTION

COMPUTER crime or a computer abuse are two general terms meaning at the same time the bad use of the technology or resulting from that bad use.

The impacts of those crimes are widely spread and many statistics reported different problems related with computer crimes and abuses and as a result of this, many countries have set laws to at least reduce these impacts.

II. WHAT IS A COMPUTER CRIME AND ABUSE

The computer crime can widely be defined as any unethical, illegal, or criminal activity or use that is directed to any information architecture. Generally, computer crime or electronic crime is that crime in which the place of the event is the computer or a network. A computer crime also involves any traditional activities like fraud, forgery, or even theft where a computer or a network is used [1]. Therefore, there are many types of computer crimes but the most crimes that widely happen are list as follows:
1- -Cyber Crime.
2-Denial of Service Attack.
3-Hacker/Hacking.
4-Computing Virus.
5-Cyber Terrorism.
6-Information Warfare.
7-Cyber Stalking.
8-Fraud and Identity Theft.

III. LAWS OF COMPUTER CRIMES

Set of rules has been globally agreed for reducing these kinds of crimes. In 1984, United States Congress introduced

Saad A. Shwaileh is with the Computer Engineering Department, KFUPM, Saudi Arabia (e-mail: s242434@kfupm.edu.sa).

The Computer Fraud and Abuse Act aiming to reduce the impacts of hacking. This law was modified later by the USA PATRIOT Act in 2001. The USA PATRIOT Act increased the scope and penalties of this act by raising the maximum penalty for violations to 10 years (from 5) for a first offense and 20 years (from 10) for a second offense. Also, by ensuring that violators only need to intend to cause damage generally, not intend to cause damage or other specified harm over the $5,000 statutory damage threshold. Additionally, it is enhancing punishment for violations involving any (not just $5,000) damage to a government computer involved in criminal justice or the military including damage to foreign computers involved in US interstate commerce. Also, in Saudi Arabia, the Saudi Legislation body which is called "Al - Shoura" has introduced set of laws to combat the growing threat of cyber crime. The laws are summarized as follows:
1- Websites distortion or defacing is considered to be a crime where the data theft could cause a fine of $ 130 thousand or even a maximum one year prison sentence.
2- Same punishment is also applied to those trying to use the internet or electronic tools for defamation or even to those trying to access private networks without permission.
3- Also, people setting up websites with pornographic unethical content or content that defames humanity, or sites with information promoting drug use may be punished with fines of up to $1.3 million and five years of jail time.
4- The largest punishment is for those trying to hack or access the governmental networks or trying to access its data and also for those people using internet for spreading terrorist views or share terrorism-related knowledge. Those people will be punished by a fine of $ 1.3 million and ten years in the prison [2]-[3].

IV. FACTS AND SURVEYS ABOUT COMPUTER CRIMES

Many studies and surveys were conducted to conclude the behavior of computer crimes around the world. One of these studies reported by the Computer Emergency Response Team of Asian School of Cyber Laws (ASCL-CERT) concluded some important statistics. The statistics were based on 6266 incidents of computer crime and abuse. That study was made for one full year started from the beginning of the January 2001 till December of 2003. This study showed that the most data were collected from information technology organizations where the least part were collected from health, telecommunication and education organizations where the other organizations' percentage ranges between 12 to 20 %. All these organizations are shown in the chart below [4] :
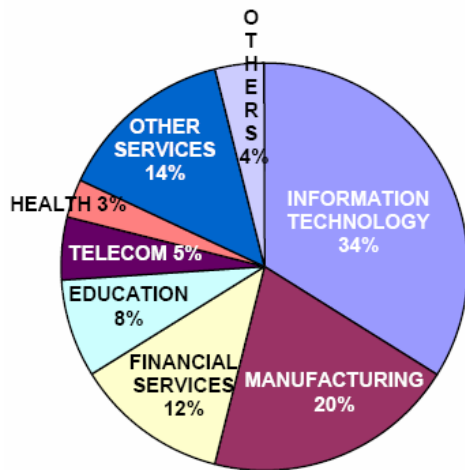
The computer crimes and abuses have been categorized into unauthorized access, data theft, email abuse, unauthorized access, data alteration, virus attacks, denial of service attacks (DoS), and others. Theses are shown below [4]:
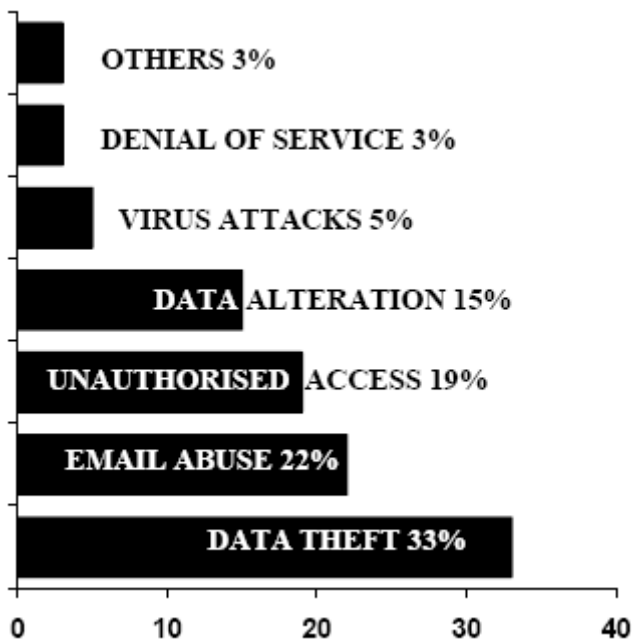
Therefore, it is obvious that the data theft is the most crime happens through hacking which will be introduced below.

In 2005, another study made by Computer Security Institute (CSI) has shown several things:

A) Financial losses resulting from hacking some security centers decreased to 61% having an average loss of $ 204,000 per respondent from $ 526,000 in 2004.

B) Virus attacks continue as the source of the greatest financial losses, accounting for 32 percent of the overall reported losses.

C) The unauthorized access has dramatically increased to 24% and has become significant crime for financial losses.

D) Theft of proprietary information also showed a significant increase in average loss per respondent; more than double that of 2004.

V. CONCLUSION

Therefore, it has been clear how computer crimes can affect people live especially for those financial crimes. Although, the information security is increased but as shown the unauthorized access for example were dramatically increased. Knowing the laws of computer crimes should be considered the first solution to reduce them.

ACKNOWLEDGMENT

REFERENCES

[1] " Computer Crime." Wikipedia 2008:
http://en.wikipedia.org/wiki/Computer_abuse

[2] " Computer Fraud and Abuse Act." Wikipedia 2008.

[3] Kornakov, Konstantin. "Cyber crime laws adopted in Saudi Arabia." Oct 2006:
http://www.viruslist.com/en/news?id=202181770

[4] " Computer Crime & Abuse Report (India) 2001-02." Asian School of Cyber Laws 2003.

[5] " 10th CSI/FBI Survey Shows Dramatic Increase in Unauthorized Access." IT Pro July/August 2005.