Chapter 5
Cyber Crimes:
Types, Sizes, Defence Mechanism, and Risk Mitigation

Hasan L. Al-Saedy
British Institute of Technology and E-Commerce, UK

ABSTRACT

The financial cost of cyber crime now has an annual cost estimated in the UK in eleven figures. In this chapter an ethic based definition of cyber crime is introduced and cyber crimes are classified. The impact of each class of cyber crime on society, individual, government and international security is highlighted. The cost of cyber crime is evaluated and a technique to prevent and mitigate the effect of these crimes on individual, government and international security and world peace is indicated. The forensic techniques and tools used in cyber crime evidence gathering and prosecuting procedure is also indicated. Finally, recommendations and suggestion are given to mitigate the impact of cyber crime on individuals, societies, world finance and international security.

INTRODUCTION

Email scam is considered as a crime in the west and the US law and regulation and probably there is no regulation in some countries to criminalize this sort of act, but this crime is ethically unacceptable in all societies worldwide, the definition could be based on the social convention or norms. Intercepting diplomatic mail by English speaking governments is an acceptable act among the five countries; however, the act is ethically unacceptable worldwide (Gurny, 2013). According to the above definition intercepted diplomatic mail is considered to be as cyber crime according what been said as agreed upon convention and norms. The recent reported case of interception of the mail of a head of European state by the US government is a violation of norm and conventions. The US constitution doesn't allow the interception of the stored or transmitted data of US citizen, in theory, without legal warrant according to the fourth amendment 'The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized'.

DOI: 10.4018/978-1-5225-7909-0.ch005

It is clear evidence that the US government security agencies are violating the privacy of the US citizens and non US citizens. Snowden revealed facts in the UK Guardian newspaper is clear evidence of the US privacy violation.

In general, cyber crimes are crimes in which the internet, computer, email and mobile are used to engineer them. The designer of this sort of crimes takes the advantages of the weak security and policy measure in networking and communications technology to implement the crime (Sanders, 1994). A wide range of cyber crimes is in use these days (Home Office, 2010). It is not possible so far to estimate the real volume of these crimes as victims are usually decline to report these crimes for many reasons. Among these reasons are cultural backgrounds and for some are for brand name protection (Schneier, 1995). However, it is possible to estimate the proportional volumes of theses crimes from governments released report (Home Office, 2010). Among the sorts of crimes are the following:

Breaching of security, copyright violation, child pornography, child grooming, computer viruses, denial of services, malicious code, financial fraud, identity theft and phishing scam. A wide used definition of crime is a forbidden and punishable act. The definition of crime as used in this article is that a crime is *ethically* unacceptable act (Mackey, 2003).

From the classes of crime mentioned above it is possible to estimate the financial cost of some and not possible to estimate a cost for others. As an example it is not possible to allocate a cost for child pornography and child grooming, this is on one hand and on the other hand it is possible to allocate a cost for email scam and phishing.

Table 1 shows the type of cyber crimes and tools used in engineering of these crimes and their implication on economy, society and world security. It is important to highlight here the following facts about the nature of research in cyber crimes, among these facts are that knowing the proportional cost of the cyber crime will help in setting the research budgets and priorities. Also setting a security plan in enterprises will help enhance the annual turnover of enterprises and again, discovering of a crime at an earlier stage will help reduce the cost of the crime (Newman, 2010).

The UK government estimate of the annual cost of cyber crimes is as much as 27 billion pounds (Cabinet Office and Detica, 2011), the cost of cyber crimes ordered from the most to the least expensive are as follows:

1. Intellectual property theft,
2. Espionage (spying),
3. Online theft,
4. Extortion,
5. Online fraud.

Figure 1 shows a histogram for the cost of the five highest crimes in cost.

(McGuire & Dowling, 2013) conducted a survey of public attitudes toward internet security in the UK environment. Table1 shows the classes of major cybercrimes, used tools and implication.

CLASSES OF MAJOR CYBER CRIMES, USED TOOLS AND IMPLICATION

The percentage of the reported crimes is very low compared with the real volumes of these crimes in all the crimes mentioned in Table 1.