Chapter 20
ICT Security Policy:
Challenges and Potential Remedies

Lawan Ahmed Mohammed
King Fahd University of Petroleum and Minerals, Saudi Arabia

ABSTRACT

Computer crime is now becoming a major international problem, with continual increases in incidents of cracking, hacking, viruses, worms, bacteria and the like having been reported in recent years. As a result of this massive vulnerabilities and new intrusion techniques, the rate of computer crime has accelerated beyond imagination. It is therefore vital to find policy of reducing and controlling the risk associated with such activities. However, unless the security challenges and countermeasures are well understood, the policy may not yield any fruitful results. This chapter discusses different categories of computer crime for the benefit of individuals and organizations concern with combating the problem. The chapter also discuses some security policies as means of limiting some of the vulnerabilities mentioned.

INTRODUCTION

In many countries, computer networks are used to control, manage and operate system services. Transportation, banking, power system, radio and television, gas, water, health services and telecommunication are highly automated and computerized. These systems, in addition to defense, government, and education form part of a society's critical information infrastructure. The vulnerability of critical infrastructure is constantly reinforced by regular media report. For instance, it was reported in (CSI, 2000a) that in October 2000, air traffic control radar systems failed for four hours, resulting in airports throughout the USA being gridlocked with grounded aircraft. In a similar report (CSI, 2000b), a hacker altered parameters on sewage pump stations causing raw sewage to overflow on the Australian Sunshine Cost in Queensland. More recently, in September 2008, online criminals compromised hundreds of pages on the BusinessWeek.com website with a SQLinjection attack (Cisco, 2008).

DOI: 10.4018/978-1-61520-847-0.ch020

Since cyber crimes very critical these days and will continue to be for the foreseeable future. It is important to find means or actions to be taken in order to reduce the impact or level of any threat. To achieve this, first we need to understand what risks, threats, and vulnerabilities currently exist in our environment. Second, we need to learn as much as possible about the problems so that we can formulate a solid response. This implies that we must develop and implement a comprehensive protection and response plan or policy in order to prevent or minimize attacks. The policy should provide response guidelines that cover every phase of an attack in the fastest, most efficient manner. Finally, we need to intelligently deploy our selected countermeasures and safeguards to erect protections around our most mission-critical assets. While there is no silver bullet to eliminate all threats, vulnerabilities and breaches, organizations can focus on addressing attacks during the most dangerous time. The costs associated with each individual attack are directly proportional to the amount of time that it takes an organization to approach the attack. Thus, the better prepared an organization is to detect, protect, and take down attacks proactively, the more likely that the organization will be able to prevent and/or recover from attacks. By trying to nip the problem in the bud, an organization can greatly reduce the amount of time wasted and money lost due to protecting the impact of a potential attack. It was reported that the Code Red Worm had caused over $2 billion in damage in 2001 (CNN, 2001). In July 2009, a report by (NewsFactor, 2009) revealed that an Internet thieves had stolen more than 289,000 Hong Kong dollars (37,000 US dollars) From Honk Kong Bank accounts.

While it may be difficult to predict precisely how technology will evolve, studying the history of telephone to Internet, mainframe to personal computer, kilobyte to terabyte, it seems reasonable to note that in the not-too-distance future, interactive computing technology, in whatever form, will be an integral and invisible constituent of our lives. In the course of doing it, the computing technology will also most definitely raise problems in relation to the security frameworks that surrounds it. The following part of the chapter examines some security policy challenges associated with computer systems in general and attempts to highlights various methods of limiting their impact. The chapter also looks into the different aspect of attacks and the various types of attack tools. Reports of vulnerabilities and hacking incidents were also given. It also discusses the impacts of such activities by reporting the cost of damages caused by cyber attackers in recent years. Some countermeasures such as recovery planning and risk management were discussed.

Security Policy Challenges

Any organization concerned about the security of its assets should have a security policy. A security policy explains the physical and logical security plan to protect the system's confidentiality, integrity, availability, and authenticity while providing an operational mechanism for secure cryptographic key distribution and non-repudiation as discussed by Schneider (2007). Realistically, many security policies are ineffective. Though, sometimes an organization gets lucky and has a security policy that is good and acceptable – but not usually. This is partly due to the challenges facing security policy. These challenges may be due to many different entities involved and different protection requirements in terms of confidentiality, integrity, access control, availability etc (Bedi, Rabia, & Shekhar 2008). A common problem with security policies is that they are too often neither instructional nor descriptive. They simply represent the rules which must be adhered to. This tends to create problems - the implementation of policies actually requires an understanding not only of the individual policies but also of the circumstances in which policy compliance is expected during day to day activities. Essentially, having the policies is only part of the equation; one also needs