Chapter 91
Management Approach of Risk Analysis in Information Security

Anca Gabriela Petrescu
Valahia University, Targoviste, Romania

ABSTRACT

This article describes how the ease of access to information and communication technologies is practically a prerequisite for the functioning of modern society. Taking the competitive market into consideration, the protection of the information infrastructure for a company, could mean that company has a competitive advantage. This article is relevant to better understand how the actors involved in information and communication technologies could develop new models of information systems and risk management strategies. The results of this research show that each manager must handle threats, because otherwise the organization's objectives cannot be met. Given that uncertainty is a fact of life, then the uncertainty response should become a permanent managerial concern.

INTRODUCTION

Information technology security threats are most often defined as being "those circumstances or events that constitute potential danger to the normal state of a communication and information system, in which the confidentiality, integrity and availability of information, resources and services are ensured" (Ministry of Communications and Information Society, 2011). Implementing appropriate security measures to counter threats such as attacks can be blocked or its effects can be mitigated.

Communication and information security incidents record a significant growth during the last years, both in number and complexity (Tiago et al., 2014; Agrawal & Tapaswi, 2017). The main motivations of large scales attacks are financial profit or political supremacy. The complex cyber-attacks in 2007 on Estonia, Lithuania and Georgia are the most widely covered examples of a general trend. The huge number of viruses, worms and other forms of malware, the expansion of botnets and the continuous rise of spam confirm the severity of the problem (Ministry of Defense Estonia, 2008).

DOI: 10.4018/978-1-7998-2466-4.ch091

Prevention means that the attack will be prevented. Typically, prevention involves implementation of mechanisms that users not be able to counteract and are implemented correctly, unaltered, so the attacker cannot alter them. Prevention mechanisms are cumbersome and often interfere with the use of the system to the point that, sometimes hamper normal use thereof. But some simple preventive mechanisms with as passwords (which are designed to prevent unauthorized users from using the system) have become widely accepted plan. Prevention mechanisms can prevent compromise of parts of the system. Once implemented, the resources protected by mechanisms not are monitored to identify any security issues, at least in theory.

Detection is particularly useful where an attack cannot be prevented, but can also indicate the effectiveness of preventive mechanisms. Detection mechanisms accepts that an attack may occur; the goal is to determine if an attack is about to occur or has occurred, and to report this procedure. However, the attack can be monitored to collect data on the nature, severity, and results. Typical detection mechanisms monitor various aspects of the system, looking for action and information indicating an attack. An example of such mechanisms is providing an alarm when the user enters the wrong password more than three times. The procedure for obtaining access to the system can be continued, but history records system audit report an unusually high number of erroneous input passwords. Detection mechanisms do not prevent compromise of parts of the system, which is a serious drawback. Protected Resources detection mechanisms must be monitored continuously or periodically to identify any security issues.

From the first two perspectives, the Romanian Strategy on Cyber Defense, drawn up by the Ministry of Communication and Information Society defines the following types of information technology security threats: information technology attacks against infrastructures that supports public utility functions or information society services that, once disrupted, may constitute a danger for social security; unauthorized access to communication and information systems and to data they handle; unauthorized modification, deletion or alteration of data in electronic format or unauthorized denial of access to such data and services; espionage by penetrating the communication and information systems of the targeted organization; inducing patrimonial prejudice, harassment or blackmail of citizens or organizations, either public or private.

According to a subject matter survey performed in the USA during 2010-2011 (Computer Security Institute, 2011), "the threats continue to mount as attacks become increasingly sophisticated and malicious". The uncertainty may take the form of either threats or opportunities. Thereby, each manager must handle threats, because otherwise the organization's objectives can not be met and capitalize the opportunities to the benefit of the organization, proving efficiency (Landoll, 2010; McQuade, 2006; He et al., 2012).

Comparing with the last five years, the survey illustrates a growth of the number of incidents caused by malicious infections from around 50% of the respondents in 2009 to around 64% in 2011, of password sniffing cases from 9% in 2009 to 17% of the respondents in 2011, of financial frauds, from 12% to 20%, of denial of service attacks from 21% to 29%, of websites defacements from 6% to 14%, as well as of theft of or unauthorized access to intellectual property that grew from around 9% to around 14% of the respondents.

Each day the society becomes more and more dependent on these information infrastructures that become a backbone of vital information flow (Ruževičius et al., 2007; Hadžiosmanović et al., 2012). Thus, the protection of this infrastructure represents a major concern of authorities all around the world. Information security has become a top of mind issue for the public, media and government (Collins & McCombie, 2012; Singer & Friedman, 2014).