Chapter 10
Risk Analysis of ICT Assets

Hamed H. Dadmarz
Independent Researcher, Iran

ABSTRACT

Risk analysis is required in all companies to help the business owners or top managers make decisions about risk management strategy, which itself provides an organization with a roadmap for information and information infrastructure protection aligned to business goals and the organization's risk profile. This chapter identifies information assets including network, electricity, hardware, service, software, and human resources in the ICT department of a health insurance company and their relevant risks. To determine the risks, the level of confidentiality, level of integrity, level of availability, the likelihood of threat occurrence, and intensity of vulnerability have been assessed and rated. Assessment is done based on the opinions of 30 experts in the field of information security. According to the results, the highest information security risk is on the network.

DOI: 10.4018/978-1-5225-7086-8.ch010

INTRODUCTION

Recently, organizations attempt to increase their information security. There are several factors that lead to an unsuitable situation of a company in the case of information security such as the lack of infrastructure and processes. Threats to information assets of a company are very different including failure or fault in a computer program, inefficient processes in planning and operation, unauthorized access, natural disaster, viruses, unprofessional human resources, misuse or abuse. Information security aims to ensure the business continuity in a structured manner and mitigate risks caused by security incidents (Labodi & Michelberger, 2010).

Although information security has been defined as a range of actions designed to protect information and information systems, it covers the entire infrastructure that facilitates the use of information. Entire infrastructure refers to hardware, software, physical security, and human factors. By increasing the number of employees, applications, and systems, the probability of vulnerability increases and it causes the management of information security harder. Nowadays, organizations depend more on information technologies and more employees do their duties by interactions with computer-based systems and therefore, there is a high potentiality of risk occurrence. This causes the importance of information security in organizations higher (Al-Awadi & Renaud, 2007).

Information security can be achieved by the protective measures and consideration of risks. These consist of risk analysis to determine assets and their relevant risk. This chapter aims to identify information assets including network, electricity, hardware, service, software, and human resources in the ICT department of a health insurance company and their relevant risks.

RESEARCH LITERATURE

Risk management is recognized as a complex activity which has many different aspects or features and involves in the entire organization. All levels of the organization from senior managers who define a strategic vision and main objectives to mid-level managers who plan, execute, and manage projects, and finally to workforces in operational level who operate with information technologies should participate in risk management (NIST, 2011). In risk identification, the degree of an organization's involvement in a critical situation is to be considered. This requires a deep understanding of the organization, the organization target market, the legal, socio-political and cultural context of that organization as well as the strategic and