Chapter 5

IT Security Risk Management Model for Handling IT-Related Security Incidents: The Need for a New Escalation Approach

Gunnar Wahlgren
Stockholm University, Sweden

Stewart James Kowalski
Norwegian University of Science and Technology, Norway

ABSTRACT

Managing IT-related security incidents is an important issue facing many organizations in Sweden and around the world. To deal with this growing problem, the authors have used a design science approach to develop an artifact to measure different organizations’ capabilities and maturity to handle IT-related security incidents. In this chapter, an escalation maturity model (artifact) is presented, which has been tested on several different Swedish organizations. The participating organizations come from both the private and public sectors, and all organizations handle critical infrastructure, which can be damaged if an IT-related security incident occurs. Organizations had the opportunity to evaluate the actual model itself and also to test the model by calculating the organization’s escalation capability using a query package for self-assessment.

INTRODUCTION

The Swedish National Audit Office (2014) concluded that the overall capacity of government agencies in Sweden to handle the consequences that can arise from serious information security incidents are largely unknown. Overall risk evaluation is currently lacking, and instead there is uncertainty as to how strong the protection is and which incidents have taken place.
IT-related security incidents in the financial sector can, for example, have a cascading effect on other sectors in the economy. If bills cannot be paid, then both production and delivery slow down and in some cases stop completely. The Swedish Civil Contingencies Agency (2014) reported that in 2011, a major IT services provider in Sweden caused an IT-related security incident that had major operational disruptions among a number of government and private organizations in Sweden.

Managing IT-related security incidents is an important issue facing many organizations in Sweden and around the world. To manage the escalation of incidents, organizations need established crisis teams with reporting channels and related report management tools that can handle incidents that do not require immediate action. This chapter presents some ongoing research work to measure an organization’s escalation capability of IT-related security incidents.

BACKGROUND AND RELATED WORKS

In this work, the term IT security risk is used to distinguish it from other business risks like investment risk, credit risk, market risk, and environmental risk. The National Institute of Standards and Technology (NIST) (2002) has proposed the following definition of risk: “Risk is a function of the likelihood of a given threat-source’s exercising a particular potential vulnerability and the resulting impact of that adverse event on the organization” (p. 8). Given this definition, IT security risks are then defined as an adverse event affecting the IT systems of an organization.

All organizations today have some kind of information system (IS) based on information technology (IT). Organizations are exposed to different threats from both inside and outside. These threats can be avoided with the help of countermeasures of different kinds. However, it is difficult to justify spending effort on countermeasures for an IT system that has little business impact for the organization. To find the right mix of countermeasures to assist organizations, several IT security risk management methods and tools have been developed.

IT Security Risk Management

IT security risk management is a part of information security management, which in turn is related to IT security governance. Different standards have been established for management and governance. The International Organization for Standardization (ISO) (2013) has established a standard for information security management that represents one of the main documents in the area. The concept of IT security governance is described in Guidance for Information Security Managers (ITGI, 2008) and in the Risk IT Framework (ISACA, 2009).

The term IT risk management refers to approaches and methods that lead to cost-effective security solutions and countermeasures (ISO 27005, 2011a). This is done by measuring the security risk to IT systems and assuring adequate levels of protection. IT security risk management is a continuous process and consists of the following main steps:

- Risk monitoring
- Risk assessment and risk treatment
- Risk communication