Chapter 65
Managing Enterprise IT Risks Through Automated Security Metrics

Aristeidis Chatzipoulidis
University of Macedonia, Greece

Dimitrios Michalopoulos
University of Macedonia, Greece

Ioannis Mavridis
University of Macedonia, Greece

ABSTRACT

Information systems of modern enterprises are quite complex entities. This fact has influenced the overall information technology (IT) risk profile of the enterprise and it has become all the more critical now to have sound information systems that can maximize business performance of an enterprise. At this point, the practical challenge for enterprises is how to manage enterprise IT risks for persistent protection of business and security goals. This chapter covers different aspects of managing enterprise IT risks, providing solutions in terms of risk management methods, automated security metrics and vulnerability scoring methods. The purpose is to introduce an in-depth study on enterprise IT risks and add value to enterprise sustainability through an extensive analysis of methods and automated security specifications.

INTRODUCTION

Information Technology (IT) risk is ambiguous and modern enterprise environments are no exception. Historically, the field of IT risk management has been dominated by theoretical discussions, practical misfits and indecipherable algorithms all of them adding to complexity and little in essence. Recent corporate failures, such as the collapse of Lehman Brothers which caused severe consequences including economic turndown and an extended systemic risk in every sector or industry, reveal the failure to identify and manage risk at an enterprise level.

DOI: 10.4018/978-1-5225-5481-3.ch065

Fact is that enterprise IT risk management has evolved but to what extent? Evolution reveals that first attempts on managing risks on enterprises started as isolated and stand-alone process before becoming fully integrated with the business processes. Figure 1 demonstrates the evolution of risk management.

First, there was the philosophy that risk should be avoided at all costs. This notion was supported by the fact that the majority of enterprises transferred business and IT risk to third party insurance companies. This notion became quickly outdated since business community started to realize that managing IT enterprise risk is not an individual responsibility and transferring risk is not a viable option. Therefore, enterprises started to align IT risk management as part of business activities with sight of managing risk rather than avoiding it. This brought up the need for IT security awareness programs and training as well as involvement of all business units. However, there were missing parts, such as governance and compliance issues. Towards this perspective, the term Enterprise Risk Management (ERM) emerged to address the limitations of previous notions, such as static risk management procedures and the need to include governance and compliance issues into a unified approach (Hampton, 2015).

Developing effective risk management strategies requires the collection of data from various stakeholders from the enterprise's environment. In turn, stakeholders started to communicate an enterprise IT risk management philosophy as means to nurture a risk-oriented culture capable to add value to the enterprise and become a proactive solution to IT risks. Towards this perspective, stakeholders should develop a high level of competence reflecting the skills and know-how to perform assigned tasks (Hoyt & Liebenberg, 2011).

Delegation is vital for a more organized and decentralized decision-making however, at the same time, this may increase the number of undesired events and affect the internal environment if individuals are not accountable for their actions. In this regard, segregation of duties (SoD) is considered a key component to maintain a strong internal control environment because it delegates responsibility to those individuals capable to accomplish a task and avoid a fraudulent activity (Taylor, 2014).

Figure 1. Evolution of IT risk management