Chapter 9

The MFC Cybersecurity Model Extension and Diagnostic toward a Depth Measurement:
E-Learning Systems Case Study

Neila Rjaibi
Institut Supérieur de Gestion de Tunis, Tunisia

Latifa Ben Arfa Rabai
Institut Supérieur de Gestion de Tunis, Tunisia

Ali Mili
New Jersey Institute of Technology, USA

ABSTRACT

This chapter presents a quantitative security risk management cybersecurity measure namely the Mean Failure Cost (MFC). We illustrate it to quantify the security of an e-Learning application while taking account of its respective stakeholders, security requirements, architectural components and the complete list of security threats. Moreover, in the mean time, security requirements are considered as appropriate mechanisms for preventing, detecting and recovering security attacks, for this reason an extension of the MFC measure is presented in order to detect the most critical security requirements to support the quantitative decision-making. Our focus is widespread to offer a diagnostic of the non secure system's problems and a depth insight interpretation about critical requirements, critical threats and critical components. This extension is beneficial and opens a wide range of possibilities for further economics based analysis. Also this chapter highlights the security measures for controlling e-Learning security problems regarding the most critical security requirements.

DOI: 10.4018/978-1-4666-8510-9.ch009

INTRODUCTION

The purpose of this chapter is to examine one among the current knowledge in the field of systems and software engineering. We address particularly the issue of the system's safety and cybersesecurity and more specifically the quantification and measure of security risk in a financial value for all the systems' stakeholders, this is the concept of risk to the security risk management approach.

This chapter focuses in general on the advancements in the engineering of systems, in particular in the software security engineering in the design or development phase of current e- systems.

In today's Internet age, E-systems are widespread and considered essential in our modern society. These systems require the sharing and the distribution of information. E-systems are vulnerable; serious security threats include software attacks (viruses, worms, macros, denial of service), espionage, acts of theft (illegal equipment or information) and intellectual property (piracy, copyright, infringement) (MohdAlwi & Fan, 2010).

Security is a current issue that needed to be addressed to ensure a safer running of systems and a higher quality. It is important to assess and to measure the security risk and its potential impact (Aissa et al., 2010 a; Aissa et al., 2012; Aissa et al., 2010 b). Research has been conducted in this perspective to improve security management approaches and models which are quantitative or qualitative. These strategies are useful to highlight the power of the security management.

Quantitative security management models are considered as a hard task in practice in order to measure the potential security risk impact caused by the attacks. But they are more useful in estimative values analyze and interpretation to provide a good plan for risk mitigation (Abercrombie et al., 2008; Mili & Sheldon, 2009).

Cybersecurity is emerging as a major concern for organizations including management systems, communication systems, critical infrastructure control, medical platforms and e-services. E-learning systems are complex given their openness, necessity, heterogeneity and widespread scope. In such systems, the danger is multiplied, and the security issue becomes an important challenge. It is of our interest to focus on the security of E-learning platforms to study their integrity, confidentiality and availability. In fact, having a stable platform without technical problems leads to a high-quality learning processes (Rjaibi & Rabai, 2011; Sun et al., 2008; Rjaibi & Rabai, 2012), competition, adequate cash, profitability and a good commercial image.

To the best of our knowledge and according to the literature review we note ignorance in addressing security topic of e-learning systems and a lack in quantitative security management models (Nickolova & Nickolov, 2007; MohdAlwi & Fan, 2010). In addition, in-depth security interpretations are also not discussed.

Our goal is to study a cybersecurity measure for the E-learning network and to schedule a deep insight and diagnostic of the critical threats, the critical architectural components and the critical security requirements. Also it is a challenging tasks, it is useful to scout about the main cybersecurity diagnostics.

This chapter highlights the definition and computation of a recent and rigourous cybersecurity measure namely the Mean Failure Cost (MFC), it computes for each stakeholder of the given system his loss of operation ($/H). This quantitative model is a cascade of linear models to quantify security threats in term of loss that results from system vulnerabilities (Aissa et al., 2010; Aissa et al., 2012; Aissa et al., 2009).