Chapter 9
Risk Assessment and Real Time Vulnerability Identification in IT Environments

Laerte Peotta de Melo
University of Brasilia, Brazil

Paulo Roberto Lira Gondim
University of Brasilia, Brazil

ABSTRACT

Contrary to static models of risk analysis, the authors propose a pro-active framework for identifying vulnerabilities and assessing risk in real-time. Instead of searching for vulnerabilities from an external point of view, where the information is obtained by simply exploring a digital asset (computational system composed of hardware and software), the authors propose that software agents (sensors) capable of providing application, configuration and location information be incorporated into assets. Any observed changes, such as physical location, software update or installation, hardware modifications, changes in security policy and others, will be immediately reported by the agent, in a pro-active manner, to a central repository. It is possible to assess risk in a certain environment comparing databases of rules and known vulnerabilities with information about each asset, collected by the sensors and stored in the central repository.

INTRODUCTION

Risk analysis may be extremely complex and is directly dependent on the proper planning and prior knowledge of the technological environment in which the analysis will be made, and as such, it is defined as a process that aims to identify, analyze, reduce or transfer risk. The technological risk analysis tools currently available in the market are highly dependent on proprietary operational systems that tie the "solution" to a single platform. Additionally, these tools base their assessment on collected information regarding past events

DOI: 10.4018/978-1-61350-507-6.ch009

and, consequently, are unable to provide a true real time solution. There is a currently growing preoccupation with information security, resulting in the growth of a new field - technology risk analysis. The role of a technological risk analyst is to identify vulnerabilities, calculate a vulnerability score and verify whether or not the identified vulnerability can potentially affect the company business. If so, he or she must correct the problem in the shortest time possible. At first glance the task seems simple, with few steps to follow; however, the number of vulnerabilities has been increasing exponentially to the point that it has become impossible to identify vulnerabilities in a manual or even semi-automatic manner.

Another point to note in risk analysis is the increasing need for transparency demanded by the market and by regulatory bodies that require corporations to follow strict information security management norms, such as Sarbanes- Oxley (SOX) (Lahti & Lanza, R. P., 2005), Basel Accords I and II, ISO 27001 (IEC/ISO, 2005), ISO 27002 (ISO/IEC, 2005) and BS-7799 (BS, 2001).

The need to adhere to international norms may result in extra costs and, in some cases, loss of competitiveness, albeit typically only in the short term. Medium and long-term effects resulting from the implementation of such norms are clearly beneficial and demonstrate a certain business "maturity" and preparedness that may even attract new investments and increase the trust of stockholders.

Information is the most valuable asset to any organization, be it for-profit or not. A successful attack targeting an organization's digital information assets can not only cause immediate financial losses but can also damage its brand image, having long term effects on its business valuation.

Information security aims at protecting digital information assets and data, guaranteeing the following basic principles:

- **Confidentiality:** ensure that information is only accessed by people or systems who have the proper authorization;
- **Integrity:** ensure that information has not been accidentally or intentionally modified, promptly detecting any unexpected alterations;
- **Authenticity:** ensure that information is genuine, *i.e.* that the party responsible for its generation is really who it claims it is;
- **Availability:** ensure that information is accessible when it is needed;
- **Privacy:** even though it is a complex concept in may be defined, in the realm of information security, as ensuring that each person to whom information is concerned has his or her individuality preserved, given that privacy requirements are usually defined by law;
- **Non-repudiation:** ensuring that a party who generates certain information cannot deny its authenticity.

RELATED WORKS

With regards to the development of this work, we did not identify any previous work that proposed to conduct a risk analysis of information assets in real time, that is to say, at the moment that vulnerability was identified and reported. In this context, we describe below the publications that contributed to meeting our original objective. The information necessary to define risk and security was established in a recent study by Perera and Holsomback. The study further suggested a matrix for risk analysis following the framework. It also provided broad definitions and discussions of the topic and incorporated views of others (literature review) into the discussion to support, refute or demonstrate its position on the topic.

The authors also proposed a risk management system based on IRMA. However, this system is limited in that risk input must always be done