A Weighted Monte Carlo Simulation Approach to Risk Assessment of Information Security Management System

Seyed Mojtaba Hosseini Bamakan, School of Economics and Management, Key Laboratory of Big Data Mining and Knowledge Management, University of Chinese Academy of Sciences, Beijing, China

Mohammad Dehghanimohammadabadi, Department of Mechanical and Industrial Engineering, Northeastern University, Boston, MA, USA

ABSTRACT

In recent decades, information has become a critical asset to various organizations, hence identifying and preventing the loss of information are becoming competitive advantages for firms. Many international standards have been developed to help organizations to maintain their competitiveness by applying risk assessment and information security management system and keep risk level as low as possible. This study aims to propose a new quantitative risk analysis and assessment methodology which is based on AHP and Monte Carlo simulation. In this method, AHP is used to create favorable weights for Confidentiality, Integrity and Availability (CIA) as security characteristic of any information asset. To deal with the uncertain nature of vulnerabilities and threats, Monte Carlo simulation is utilized to handle the stochastic nature of risk assessment by taking into account multiple judges' opinions. The proposed methodology is suitable for organizations that require risk analysis to implement ISO/IEC 27001 standard.

Keywords: *Analytic Hierarchy Process (AHP), Information Security Management System (ISMS), ISO/IEC 27001, Monte-Carlo Simulation, Risk Assessment*

INTRODUCTION

In today's competitive business environment, information has a key role in any organization. Hence protecting, securing and managing information appropriately are crucial (Kritzinger & Smith, 2008). In last few decades, many firms completely were tied to information systems to handle their daily process with the lowest labor cost, materials and capital, and in return, gain more appropriate and efficient services. However, information security threats could jeopardize the information and must be given serious attention by organizations (Ou Yang, Shieh, & Tzeng, 2013). Information violation would negatively affect the organization by: losing time, manpower,

DOI: 10.4018/IJEIS.2015100103

money and business opportunities. So protection of information is called information security (Kritzinger & Smith, 2008) which has been considered as a predominant topic of information system development (Zhiwei & Zhongyuan, 2012). Keeping the information secure through managing the information security risks, threats and vulnerabilities can be defined as an information security management (Kritzinger & Smith, 2008). Since information systems are growing through businesses, it brings more costly consequences because of information system security infringement (Feng, Wang, & Li, 2014).

The main objective of the information security is to protect the availability, confidentiality and integrity of the information (Aljifri & Sánchez Navarro, 2003; Kritzinger & Smith, 2008). Different factors such as human factor, education and technology add complexity to the information security processes (Yeniman Yildirim, Akalp, Aytac, & Bayram, 2011). Information security risks can occur as technical failures, system vulnerabilities, human failures, fraud or external events. Hence, developing an information security systems to protect the confidentiality, integrity and availability of information assets, is a strategic goal for organizations (Bojanc & Jerman-Blažič, 2008).

As a crucial part of information security systems, *security risk analysis* is focused on how to measure and analyze vulnerabilities and threats of information assets and then keep risk at an acceptable level by using appropriate controls. Since organizations are in a complex and dynamic environment, security risk analysis could be very challenging (Feng et al., 2014). A variety of international information system guidelines have been developed including ITIL, CobiT, ValIT, TCSEC/Orange Book, IT Baseline Protection Manual, Generally Accepted Information Security Principles (GAISP), the System Security Engineering CMM (SSE-CMM), and BS7799 (Siponen & Willison, 2009). Among these alternatives, the standard ISO/IEC 27001:2005 has received more attention because of its flexibility in implementation and has been utilized by in both commercial and government sectors with different sizes: small, medium and large organizations (Humphreys, 2008). This Information Security Management System (ISMS) framework is a risk-based information security standard. This standard enables organizations to assess risky information assets and reduce the risk level of them by allocating any of the security controls that are listed on ISO/IEC 27001's Annex A.

Although risk assessment and management are the primary element of standards such as, ISO/IEC 27001 and 27002 (ISO/IEC27001, 2005; ISO/IEC27002, 2005), these standards do not propose any well-defined methodology for risk assessment. There are many different risk assessment methodologies with their own advantages and disadvantages (Shamala, Ahmad, & Yusoff, 2013), however there is no agreed upon reference benchmark or comparative framework to consider one risk assessment method better than the others (Saleh & Alfantookh, 2011; Shamala et al., 2013; Syalim, Hori, & Sakurai, 2009). Some of these methodologies are qualitative, while some others are quantitative in nature (Saleh & Alfantookh, 2011; Shamala et al., 2013) or combination of both (Feng & Li, 2011; Feng et al., 2014). Due to the differences in goals, steps, structures and levels of application, they will be used in different situations. However, context establishment, risk identification and risk analysis are the three common steps in a general information risk assessment process (Shamala et al., 2013).

The proposed method by ISO/IEC 27001 suffers from few shortcomings. For instance, all the metrics are static, while due to the inherent uncertainty of events, the chance of a risky event occurrence is usually probabilistic. Additionally, in case of experts' disagreement, this standard does not provide any suitable solution. Moreover, there is not a straightforward method for weighting the CIA (Confidentiality, Integrity and Availability) measures. As a result, this paper aims to address these issues by proposing a novel method which follows this goals: