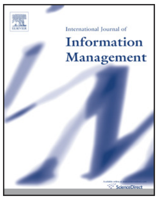
Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt



# Information security risk analysis model using fuzzy decision theory

Ana Paula Henriques de Gusmão*, Lúcio Camara e Silva, Maisa Mendonça Silva, Thiago Poleto, Ana Paula Cabral Seixas Costa

*Management Engineering Department, Universidade Federal de Pernambuco, P.O. Box 7462, 50722-970 Recife, PE, Brazil*

ARTICLE INFO

*Article history:*
Received 29 July 2015
Received in revised form 6 September 2015
Accepted 12 September 2015
Available online 26 October 2015

*Keywords:*
Information security
Risk analysis
Fuzzy decision theory

ABSTRACT

This paper proposes a risk analysis model for information security assessment, which identifies and evaluates the sequence of events – referred to as alternatives – in a potential accident scenario following the occurrence of an initiating event corresponding to abuses of Information Technology systems. In order to perform this evaluation, this work suggests the use of Event Tree Analysis combined with fuzzy decision theory. The contributions of the present proposal are: the development of a taxonomy of events and scenarios, the ranking of alternatives based on the criticality of the risk, considering financial losses, and finally, the provision of information regarding the causes of information system attacks of highest managerial relevance for organizations. We included an illustrative example regarding a data center aiming to illustrate the applicability of the proposed model. To assess its robustness, we analyzed twelve alternatives considering two different methods of setting probabilities of the occurrence of events. Results showed that deliberate external database services attack represent the most risky alternative.

## 1. Introduction

According to Kiyomoto, Fukushima, and Miyake (2014), Information Technology (IT) systems consist of computing resources and networks, which support the performance of critical functions in organizations. Moreover, IT systems have improved how business is executed, making organizations more dependent on their computer systems (Magklaras & Furnell, 2002).

However, despite the benefits and advantages of IT systems, many issues regarding IT infrastructure exhibit security flaws that render them susceptible to abuse.

Security abuses, according to Bojanc & Jerman-Blazic (2008), are related to technical failures, system vulnerabilities, human failures, fraud, and external events. Financial losses are often a consequence of security abuse (Sun, Srivastava, & Mock, 2006). Rasheed (2014) reported many companies identifying security concerns as the remaining barrier to adopting cloud computing services and Brender and Markov (2013) claim that those risks need to be carefully evaluated before any engagement in this area. Thus, the IT industry has provided a variety of security tools (e.g., anti-virus and firewalls) that help users and system administrators prevent, detect, and counteract IT abuse, according to Magklaras and Furnell (2002).

Information security has become crucial to the survival of institutions. Thus, several security solutions have been developed to minimize risks that endanger organizations' operations and to maintain the confidentiality, integrity, and availability of information. These solutions mainly focus on analysing vulnerabilities and threats to the IT systems and deciding what countermeasures reduce risk to an acceptable level (Feng, Wang, & Li, 2014). However, these solutions are not simple tasks due to the complex and dynamic environment.

This same assessment is pointed out in Feng and Li (2011), in which information system security (ISS) risk analysis is a difficult task and involves uncertainty, which is considered to be the main factor that influences the effectiveness of the ISS risk assessment. However, these authors also argued that several existing approaches for ISS risk analysis have some difficulties in dealing with the uncertainty. To overcome this problem, considering the uncertainty inherent to the context, this paper developed an approach that combines decision theory and fuzzy logic by incorporating the vision of the work developed by Shamala, Ahmad, and Yusoff (2013), which not only identified and ranked potential systems vulnerabilities but also identified and monitored specific threat levels of deliberate and external data center attacks.

Therefore, the objective of this paper is to assess the risk, which is the first step in the risk management methodology for information technology systems (NIST, 2002). The risk assessment, in

* Corresponding author. Fax: +55 81 21268728.
*E-mail addresses:* anapaulahg@hotmail.com (A.P.H. de Gusmão), luciocsilva@gmail.com (L.C. e Silva), maisa.ufpe@yahoo.com.br (M.M. Silva), thiagopoleto@hotmail.com (T. Poleto), apcabral@ufpe.br (A.P.C.S. Costa).

http://dx.doi.org/10.1016/j.ijinfomgt.2015.09.003
0268-4012/© 2015 Elsevier Ltd. All rights reserved.

turn, encompasses nine primary steps: System Characterization, Threat Identification, Vulnerability Identification, Control Analysis, Likelihood Determination, Impact Analysis, Risk Determination, Control Recommendations, and Results Documentation. The event tree analysis (ETA) methodology in this paper will support the step of System Characterization through the identification of the vulnerabilities of the organization and consequently, the potential accidents and possible scenarios. The Risk Determination step will be supported by decision theory and fuzzy logic through determination of the chances of occurrence and judgments about these elements. Thus, this article proposes the use of specific methodologies in crucial stages of risk assessment in information security. Both mathematical rigor, which is necessary to ensure the robustness of the model, and the judgments of those involved in the process, given the subjective characteristic of the types of assessments made, are considered in this model. In this way, this new approach of dealing with information security in IT systems enables managers to better understand the problem by estimating the level of threat that is likely to originate from a particular scenario in an uncertain environment.

The first section of the paper discusses information security risks in IT systems. Then, a discussion follows of the existing methodologies on information security and the background information necessary to develop the proposed approach. Next, we introduce the methodology and present a real case illustrating how the methodology validates the proposed approach. Finally, the discussion turns to limitations of the research, suggested further studies and concluding remarks.

## 2. Background

### 2.1. Information security risk analysis

This section presents a brief summary of related works in information security risk management models. The necessity of information security in organizations has increased as huge changes in structure and type of information technologies implemented have generated greater risk (Shamala et al., 2013). As a result, several risk management frameworks and methodologies in information security literature have been developed.

Lo and Chen (2012) compared the advantages and disadvantages of qualitative and quantitative methods used in risk assessment. Quantitative methods, while providing higher accuracy with respect to risk assessment, have the disadvantage of difficulty of obtaining data. On the other hand, the qualitative method, i.e., working with judgments, intuition and experience, provides subjective assessments that are questionable in most cases. In this sense, much research has been done on fuzzy methods intended to diminish the subjective nature of qualitative risk assessments (Liu, Dai, Wang, & Ma, 2005; Wang, Chao, Lo, Huang, & Younas, 2007).

According to Paula and Vignon-Davillierb (2014), most traditional security risk management approaches involve the identification of information assets, followed by the identification and evaluation of risks with respect to those assets. Silva, Gusmao, Poleto, Silva, and Costa (2014) developed an approach that encompasses failure modes and effects analysis (FMEA) and fuzzy theory, and which analyses five dimensions of information security: access to information and systems, communication, infrastructure, security management, and security information systems development. Magklaras and Furnell (2002) proposed an approach that estimates the level of threat likely to originate from a particular insider by introducing a threat evaluation system based on certain profiles of user behavior. Considering the Computer Crime and Security Survey of the Computer Security Institute (Power, 2001), which reports that 49% of the respondents faced IT security incidents due to the actions of legitimate users, Magklaras and Furnell (2002) presented a new, innovative approach of dealing with insiders that abuse IT systems. However, their focus is only to identify possible internal threats. External factors and even other internal factors, dissociated from human actions, are not considered. The same focus is given in Schultz (2002) and Theoharidou, Kokolakis, Karyda, and Kiountouzis (2005).

Feng and Li (2011) proposed an Information Systems Security (ISS) risk assessment model based on the improved evidence theory. The advantages of the model related by the authors are: the model is based on evidence theory, which can effectively model the uncertainty involved in the assessment process; the model provides a new way to define the basic belief assignment through a fuzzy measure, which allows it to deal with fuzzy evidence found in the ISS risk assessment; the model provides a method of testing the evidential consistency, which can reduce the uncertainty derived from the conflicts of evidence provided by experts. The difficulty with relation to the use of this model resides in experts' judgment elicitation.

In contrast, Shamala et al. (2013) proposed a conceptual framework of information structure for Information Security Risk Assessment (ISRA) that supports organizations in making security-planning decisions and enables managers to design precise plans for the ISRA process. This framework clarifies the general view of information flow, types of information to collect, and requirements to be met before any risk assessment is conducted. Nevertheless, this work does not propose any new risk analysis methodology based on the comparisons made among six methodologies of ISRA. Recognizing this weakness, the authors assure that they will conduct further research based on quantitative and qualitative methods to make the infrastructure more complete and detailed for information security assessment in all types of organizations.

Feng et al. (2014) proposed a Security Risk Analysis Model (SRAM) based on Bayesian networks and ant colony optimization. This model deduces the occurrence probabilities and consequence severities of security risks and then calculates the vulnerability propagation paths using ant colony optimization to provide guidance for developing security risk treatment plans. However, as reported by the authors, the treatment of uncertainty should be considered by the SRAM in future works: introducing fuzzy sets into the model for example. This concern results because, for many, security risk analysis is quite complex and full of uncertainty (Alter & Sherer, 2004).

Also, according to Bojanc and Jerman-Blazic (2008), some researchers, like Anderson (2001), Anderson and Schneier (2005) and Schneier (2004) have realized that information security is not a problem that only technology can solve and have tried to include an economic point of view. In this way, which is different from other methodologies, the proposed model aims to evaluate the consequence of each of the alternatives of potential threat in terms of financial loss, since this is generally used and perceived by decision makers, considering the different possible events (possible nature of these threats). For the evaluation of the scenarios, the use of ETA methodology is proposed and the evaluation of the alternatives is based on decision theory and fuzzy logic. These concepts are briefly introduced in the following sections.

### 2.2. A review on event tree analysis methodology

According to Clifton and Ericson (2005), ETA is an analysis technique for identifying and evaluating the sequence of events in a potential accident scenario following the occurrence of an initiating event.

Bidder et al. (2014) describes ETA as a diagrammatical representation of the 'system', whereby the system includes the